Title	Legislation	Subject area	Body
192.com Standard letter	DPA	Internet & technology	Before 2002, the Representation of the People (Amendment) Regulations 1990 placed local council Electoral Registration Officers under a duty to sell copies of the electoral register to anyone who wished to buy them. This meant that before 2002 commercial companies could legally obtain the entire electoral roll to use for their own purposes. Our long held view was that the sale of the entire electoral roll to anyone prepared to pay for it was inconsistent with the requirements of the Act and the Human Rights Act 1998. As individuals are legally required to supply personal information to Electoral Registration Officers, we considered that extra, non-electoral uses of this information should be kept to a minimum. A related court case in 2001 confirmed this view. Following this court judgement, the Representation of the People (Amendment) Regulations 2002 were introduced. These new regulations meant that from the 2002 electoral roll canvass there were two versions of the register, a full and an edited version. Everyone who provides their details is included in the full register which is only available for certain statutory purposes (such as electoral purposes) and to credit reference agencies. However, as you may be aware, when individuals now provide their details for the electoral roll the forms contain an option to choose whether or not your name should also be included on the edited register. The edited register is now the only register available for general sale. It is my understanding that 192 only publishes personal data taken from the pre 2002 rolls and post 2002 edited rolls. There are a number of current websites which provide search facilities based on electoral rolls collected since the change to the law in 2002 i.e. electoral rolls where individuals have had the option to decide whether their details should be included in the publicly available version or not. The use of these limited versions of the electoral roll for each year since 2002 on an online search facility of this nature is not likely to breach the requirements of the Data Protection Act 1998. I can see from your correspondence that you have asked 192.com to remove the information from their site. For us to look at a complaint regarding this then we would need to see that you have completed the CO1 form that can be found on the website. If you have completed this form already and can send us a copy evidencing when the form was sent then we may be able to look at a complaint regarding your concern.

			If you have not already completed the form a link can be found below. http://www.192.com/misc/privacy-policy/ I can see from your correspondence that you have asked 192.com to remove the information from their website. For us to look at a complaint regarding this then we would need to see that you have completed the CO1 form that they require before they will remove any details. If you have completed this form already and can send us a copy evidencing when the form was sent then we may be able to look at a complaint regarding your concern. If you have not already completed the form a link can be found below. http://www.192.com/misc/privacy-policy/ Co1 Form
1st Principle DPA - Fair and lawful	DPA	Other	The interpretation of the first principle can be found in schedule 1 part II (1-4) What the Act Requires: When deciding whether or not the processing of personal data is fair, the way in which the personal data was obtained needs to be considered, In particular, whether any person from whom the personal data are obtained is 'deceived or misled' regarding the purpose(s) for which the data are to be processed. The sch. 1, part II interpretation of the first principle requires that where data are obtained from Data Subjects the Data Controller provides specific information. The DPA states that a data controller: 'must ensure, so far as practicable that the Data Subject is provided with, or has made readily available to him the following information, at the point where the data are to be collected:The identity of the Data ControllerIf they have nominated a representative for the purposes of the Act, the identity of that representative.The purpose or purposes for which the data are intended to be processedAny further information which is necessary, taking into account the specific circumstances of how the data are to be processed to ensure the processing in respect of that data is fair. E.g. the Data Controller should consider what processing of personal data they shall carry out once the data are obtained, consider whether or not Data Subjects are likely to understand the purposes for which the personal data are to be processed, the likely consequences of such processing and non obvious disclosures of data.'

4th principle DPA - Accuracy of Health Records	DPA	Health	The fourth principle of the Data Protection Act 1998 states that: 'Personal Data shall be accurate and where necessary, kept up to date'. In terms of the Data Protection Act 1998 ' accuracy' means factual accuracy. In the context of the Act, "inaccurate" means incorrect or misleading as to any matter of fact. If personal data can be proven to be factually inaccurate, then the data subject can write to the data controller to request them to correct such data. The Act goes on to state that data controllers will not be regarded as being in breach of the Fourth Principle in cases where the data controller has taken reasonable steps to ensure the accuracy of the data and, where the data subject has advised the data controller that he or she disputes the accuracy of the data, the data indicate this fact (usually by the data controller placing a note on file to this effect). However, it is important to note that health records will contain medical diagnoses made by a health professional and these represent the opinions of medical professionals. The ICO has issued a guidance note for organisations on this topic which explains best practice in the recording and retaining of professional opinions:- How does the Data Protection Act apply to professional opinions? As explained above, if a data controller receives a challenge to the accuracy of a professional opinion, they are advised to put a note on the record explaining this, rather than deleting the opinion/diagnosis. It is important to note that:-Disagreeing with an opinion is not the same as being able to dispute the accuracy of information;Where a professional opinion has been provided the ICO would not be able to dispute its validity and the complaint should be made direct to the person who expressed the opinion, or to any regulatory body overseeing their activities. If a data controller refuses to add an individual's comments to the record after receiving an adverse assessment, the ICO would not be in a position to compel them to do so. Therefore, the only practical option for the permanent deletion of the disputed information may be for the individual concerned to pursue the matter through the County Courts under Section 14 of the Act. "14 – (1) If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data"…

6th principle DPA - Rights of data subjects	DPA	Other	A person is to be regarded as contravening the sixth principle if, but only if— (a)he contravenes section 7 (the right of subject access) by failing to supply information in accordance with that section, (b)he contravenes section 10 (the right to prevent processing likely to cause damage and distress) by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section, (c)he contravenes section 11 (the right to prevent processing for the purposes of direct marketing) by failing to comply with a notice given under subsection (1) of that section, or (d)he contravenes section 12 (the right in relation to automated decision-taking) by failing to comply with a notice given under subsection (1) or (2)(b) of that section or by failing to give a notification under subsection (2)(a) of that section or a notice under subsection (3) of that section.
7th principle DPA - Destruction of personal data	DPA	Other	The Data Protection Act 1998 does not give any specific guidance on how to dispose of personal data, e.g. the Act does not mention shredding etc. However the 7th Principle states: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. Therefore, when deciding what measures to take in relation to the 7th principle, particularly in terms of disposing of data, the data controller must take into account the nature of the data and the harm that might result from any unlawful processing or loss of that data. In other words the method of destruction of personal data should be appropriate to the data concerned, in all cases it would be appropriate to ensure that the data was disposed of in such a way that there would be little risk of the data being able to be used by an unauthorised third party to the detriment of the data subject. However how this is specifically achieved is left to the discretion of the Data Controller.

7th Principle DPA - Security	DPA	Other	The interpretation of the seventh principle - schedule 1 part II (9 - 12) 9 Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to— (a)the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and (b)the nature of the data to be protected. 10 The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data. 11 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle— (a)choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and (b)take reasonable steps to ensure compliance with those measures. 12 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless— (a)the processing is carried out under a contract— (i)which is made or evidenced in writing, and (ii)under which the data processor is to act only on instructions from the data controller, and (b)the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

8th Principle DPA - Countries with adequacy	DPA	Other	The 8th principle does not allow personal data to be transferred from an EEA based data controller to a data controller in those countries without adequacy. (Exceptions apply). EEA COUNTRIES (no restrictions on transfer): Austria - Belgium - Bulgaria - Croatia - Cyprus - Czech Republic - Denmark - Estonia - Finland - France - Germany - Greece - Hungary - Iceland - Ireland - Italy -Latvia - Liechtenstein - Lithuania - Luxembourg - Malta - Netherlands - Norway –Poland - Portugal - Romania - Slovakia - Slovenia - Spain - Sweden ADEQUATE COUNTRIES: Andorra - Argentina - Canada - Faroe Islands - Guernsey - Isle of Man - Israel - Jersey - New Zealand - Switzerland - Uruguay ADEQUATE COUNTRIES – Air Passenger information only: Australia Gibraltar On entry to the European Union in 1973 Gibraltar was the ONLY British Overseas Territory that joined the EU as part of the UK's entry. As such Gibraltar has 'adequacy' under the 8th principle. However, they do have their own DPA laws which derive from the EU directive and an authority to oversee them. External links Safe Harbor website: http://www.export.gov/safeharbor/ Adequacy information and findings on European Commission website: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

8th Principle DPA - Embassies	DPA	Government - central	Line to take for transfers to UK embassies overseas The ICO has previously assumed that embassies (which includes, high commissions and consulates) are on sovereign soil of the country of origin (ie the UK) based in the host nation (ie the U.S). As such, any transfer of personal data would effectively be like sending personal data within the UK. Therefore the 8th principle does not apply in these cases. However this assumption is slightly incorrect. According to the FCO, Embassies are not part of the UK. However, personal data is protected in two ways: a) the Embassy is inviolable. That means that the authorities of the host state have no right of access to the premises of the embassy, and the property within the embassy; and b) UK embassies apply the UK Data Protection Act regardless of where they are located and the citizens with whom they deal. Given the confirmed status of the Embassy not being part of the UK or on sovereign soil, the 8th principle applies to any transfers to UK embassies in third countries, and so an organisation still needs to carry out an adequacy assessment for their transfer. With the above information, however, it should be straightforward for an organisation to come to a positive adequacy assessment for their transfer. Line to take for transfers to foreign embassies in the UK A situation may arise where a UK citizen has to send personal data to a foreign embassy but within the UK. Again, given that the embassy, whilst not foreign soil, will apply the data protection principles of its own territory or country. Therefore citizens or organisations should ensure that they comply with the 8th data protection principle when transferring personal data outside the EEA. Ian Williams - 25/07/12

Access to Adoption Records	DPA	Health	Background This line to take has been developed with regard to complaints and enquiries relating to attempts to gain access to adoption records under the subject access provisions of the DPA. Where we receive enquiries and complaints relating to tis issue, they are most commonly received from individuals who have been unsuccessful in their application to become adoptive parents. Line to take When looking into the issue of compliance with the subject access provisions where the personal data requested consists of adoption (or 'parental order') records and reports, we must take statutory instrument 419 into account. This statutory instrument is entitled 'The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (no.419)'. In effect, the statutory instrument provides an exemption where the withholding of the data in question is deemed necessary 'in the interests of safeguarding the interests of the data subject himself or the rights and freedoms of some other individual' (the 'other individual' typically being the child being considered for placement with a family). The explanatory note at the end of the statutory instrument refers specifically to 'information contained in adoption and parental order records and reports' as being appropriate to consider for exemption.

Access to copies of a credit agreement, original signed copy, or bank statement.	DPA	Finance	Borrowers and hirers are able to ask creditors to send them information about their credit agreements. If information is not provided within 12 working days, the debt becomes unenforceable until they get the information they asked for. Sections 77, 78 and 79 of the Consumer Credit Act 1974 outline the information creditors must provide to debtors under fixed-term, running account and hire agreements. Under these sections a debtor can pay £1 to get:a copy of their agreementcopies of some of the other documents mentioned in their agreementa statement of account. If this information is not provided within 12 working days the debt becomes unenforceable. This means a creditor: •cannot: - make the debtor pay the debt before they're supposed to - get a court judgment against the debtor - take back anything hired or bought on credit, or take anything used as security in the agreement. •can: - ask debtors to pay what they owe - send a default notice - pass information on to a credit reference agency - pass information on to a debt collector - sell the debt to someone else - take the case to court. NB Even under the CCA, there is no obligation to provide a signed copy of the original agreement, only a copy. This is because sections 77 and 78 of the CCA state that a creditor must give a consumer a copy of their executed agreement within 12 working days of receiving a request in writing and the appropriate fee. The Consumer Credit (Cancellation Notices and Copies of Documents) Regulations 1983 (“CNCD”) specify that every copy of an executed agreement, security instrument or other copy referred to in the CCA and delivered or sent to a debtor, hirer or surety under any provision of the Act shall be a true copy thereof. However, it is well established that a “true copy” is not an exact copy. Regulation 3(2) of the CNCD Regulations allows the following to be omitted from any copy:

			a) Information in the original which relates to the debtor, hirer or surety or is included for the use of the creditor or owner only and which is not required to be included in the original agreement by the Act or by any regulations as to form and content. Therefore it is not necessary for the copy to reproduce, for example, details of the business or occupation of the debtor, the name and address of the employer or bank details of his income etc, b) Any signature box, signature or date of signature. Therefore there is no requirement for a company to send a requester a copy of the original agreement. They may simply send the requester a copy of the terms and conditions of the agreement. Further to this, sections 77 and 78 of the CCA do not apply once the agreement has ended; therefore a creditor does not have to supply a requester with a copy of the agreement if the credit has been repaid. Bank statements In principle, a SAR for a bank statement is no different to a standard SAR. However, the DPA only compels a Data Controller to supply a copy of the personal data to the data subject. In terms of requests for bank statements, a Data Controller could comply with the SAR by providing a computer printout of the individual's transaction information which would contain the same information as the bank statement. Most lenders will charge their own fees for supplying specific duplicate bank statements, often over and above the SAR standard fees. Therefore, when making a SAR for bank statement information to a lender, a data subject should be aware that they may receive a copy of their transaction information rather than actual duplicates of the monthly bank statements that they may have previously been sent, unless they are willing to pay for the service, rather than just paying the £10.00 SAR fee.
Access to Court Records	DPA	Police, legal & criminal justice	How do I access court records? Individuals can access court documents through the court for a court specific per page fee. If the documents are made available through this route then Section 34 of the DPA applies. This section states that information made available to the public by other legislation is exempt from subject access and the non-disclosure provisions of the DPA. This means that documents made available to an individual through the court cannot be requested through subject access under the DPA. However, if the court refuses to provide documents through their own access regime, then at that point section 34 would cease to apply as the information requested is now not available to the public under other

			legislation. In these circumstances an individual could make a subject access request to the court for a copy of their personal data. To make a subject access request the individual would have to write to the court asking them for a copy of the personal information that they held. The court could then charge a maximum of £10 to comply with a request and they would have 40 calendar days to respond. However, there are a number of exemptions within the DPA that mean that the court may be able to withhold some (or all) of the individual's personal data. There is also the issue of whether the information in court records is in a relevant filing system or whether it is personal data at all.
Access to deceased persons' medical records	DPA	Health	The Data Protection Act does not provide a right of access to deceased persons' medical records. Some individuals may have a right to access a deceased person's data through the Access to Health Records Act 1990 where the information is held by a GP/Hospital. This legislation is regulated by the Department of Health. For information about the Access to Health Records Act 1990, individuals can contact the Department of Health (www.doh.gov.uk). Further guidance is also available from the NHS Choices website:- http://www.nhs.uk/chq/Pages/access-to-medical-or-health-records-of-someone-who-has-died.aspx NB The Access to Health Records Act will not allow individuals to obtain care records relating to deceased persons held by care homes/social services etc.

Access to information held by schools - maintained schools	DPA	Education	It is important initially to differentiate between a request for educational records held within the state system (which is 15 school days to respond) and subject access (which is 40 calendar days). Any complaints about access to educational records held within the state system are not DPA issues. These should be raised with the Governing Body, then Local Education Authority and then the Department for Education. If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days. The maximum amount that can be charged for dealing with the request depends on the number of pages of information to be supplied. See the SAR COP for more information. Educational records It is important to emphasise that the pupil information regulations provide **parents (or those with parental responsibility)** with a right to access the **educational records** (as defined) of any child for whom they are legally responsible. The education record must be provided within **15 days**. DPA In contrast, the DPA provides **an individual** in education with a right to ask their educational establishment for a copy of **all the personal data** relating to them held by the establishment. A parent may only use the DPA to access information held by the educational establishment about their child where the child is insufficiently mature to make his/her own subject access request or where the child asks the parent to make a request on their behalf. In making a subject access request for their child's personal data, a parent will be acting as the child's **authorised representative** and, subject to any DPA restrictions or exemptions, will be entitled to receive on the child's behalf, all personal data that establishment holds in relation to the child. The personal data is to be provided promptly and in any event within **40 days**. The parent is only legally authorised to exercise section 7 DPA rights on behalf of the child where the parent is acting for the child and in the child's best interests. There is a presumption that a parent will be acting in the child's best interests but this presumption may be **rebutted** where the data controller has reason to believe that the parent is acting in their own interests (rather than the child's) in seeking to access the child's personal data. This is in contrast with the parent's right to access the child's educational record under the regulations which is a straightforward statutory right of the parent that does not need to be exercised in the child's interests. Which pupil information regulations are currently in force?

			The pupil information regulations under which parents of children at maintained schools in England, Wales and Northern Ireland can access their child's educational records are as follows:-Education (Pupil Information) (England) Regulations 2005Education (Pupil Information) (Wales) Regulations 2004 (as amended)Education (Pupil Reporting) Regulations (Northern Ireland) 2009 In Scotland, unlike the rest of the UK, the parental right of access to the pupil record does include the independent sector. The relevant regulations are as follows:-Pupils' Educational Records (Scotland) Regulations 2003. Where is the definition of an "educational record" in the pupil information regulations? "Educational records" for England are defined in the pupil information regulations which are available through this link: Regulation 3 of the 2005 Regulations. How does the age of the child affect access to their personal data? In England, the 2005 pupil information regulations do not refer to a child's age in relation to requests, but only in respect of the head teacher's annual report, which can be provided to a pupil aged 18 (regulation 6). This suggests that parents may make a request under the regulations even where the pupil is 18. A pupil who has capacity (who might be aged 12 or over) may make a SAR to the school in respect of him or herself under the DPA, but not under the pupil information regulations.
Access to information held by schools - non-maintained schools	DPA	Education	The advice below relates to academies and free schools in England because there are no free schools or academies in Scotland, Wales or Northern Ireland (NB whilst there may be schools that have 'academy' in their names, they are not constituted as academies in the English context). Summary Independent schools have never been covered by the Education (Pupil Information) (England) Regulations 2005 so parents have not been able to apply for a copy of their child's "educational record". Academies and free schools are types of independent school and therefore parents cannot access their child's "educational record" from these schools either. However, in most cases academies and free schools will be subject to The Education (Independent School Standards) (England) Regulations 2010 which include a requirement that an annual written report of each pupil's progress and attainment in the main subject areas taught is sent to the parents except where the parent has agreed otherwise. Other personal information is available via a SAR as usual.

			Detail An academy is a publicly-funded independent school rather than being a maintained school which is funded by central government through the local authority. A free school is essentially a type of academy (their set-up involves an academy trust entering into academy arrangements with the Secretary of State for Education) which therefore means they are a type of independent school. In most cases, academies and free schools will be subject to independent school regulations as they would fall within the definition of an independent school that is given in the Education Act 2002. **In England**, The Education (Independent School Standards) (England) Regulations 2010 include a requirement that an annual written report of each pupil's progress and attainment in the main subject areas taught is sent to the parents except where the parent has agreed otherwise (see previous section for further detail). **In Wales**, The Independent School Standards (Wales) Regulations 2003 – provides for annual report to parents on the child's education, plus copy of any inspection reports. It does not appear to give any rights to parents to have ad hoc reports on their child's performance. NB- **In Northern Ireland**, The NI Department of Education processes applications and registrations for independent schools in NI, which is a legal requirement under Article 38 of theEducation and Libraries (Northern Ireland) Order 1986 and the Independent Schools (Registration) Regulations (Northern Ireland) 1974. This legislation has no effect on the provision of information by indipendent schools to pupils or parents.
Access to Land Registry information.	DPA	Government - central	Background The Land Registry makes records including some personal information available to third parties for a fee. Our understanding is that the documents are made available to ensure that purchasers can establish proper title when purchasing property. In practical terms this means that a purchaser can check that the vendor does in fact own the property they are offering for sale. Therefore we are of the opinion that in making certain information available, the Land Registry are not likely

			to be breaching the DPA. Line to takeThe land register and the documents filed with Land Registry together form a public register under the Land Registration Act 2002. Sections 66 and 67 of this Act require the Land Registry to ensure these documents are available for public inspection.As a public register the personal information held by the Land Registry is covered by section 34 of the Data Protection Act and is exempt from the non-disclosure provisions. It is therefore not a breach of the Act to release this information – even though this may include personal information.The Land Registry have assured us that documents showing personal information cannot be viewed on its website unless the £3.00 fee has been paid.Anyone can apply for copy documents relating to mortgages, which will include a borrowers name, address and signature. Mortgage references are also included by some lenders but these are not the same as bank account numbers and are unlikely to allow anyone access to an individual's bank account. These copy documents will be made available for a small charge (£3.00).Section 66 and 67 of the Land Registration Act make such disclosures compliant with the DPA by virtue of section 34 of the DPAAll copy documents of this type must come complete with signatures otherwise they will be invalid and not be acceptable for their intended purpose, for example to illustrate that a mortgage or other credit arrangement has been made in respect of a particular property.The Land Registry do have a procedure which can be used to request that confidential information is edited out of a document before a copy is supplied. Individuals would need to show that the information, if disclosed, would be likely to cause substantial unwarranted damage or distress, or to prejudice commercial interests. But that exemption could later be challenged and, if the registrar then decided that disclosure was not damaging or prejudicial or that disclosure was in the public interest, he would release the unedited document.In order to be able to rely on this procedure, a property owner would need to make a clear case that damage or distress was likely; the fact that the owner would prefer the information not to appear would not be a sufficient reason for Land Registry to withhold it.
Access to proof of partners' convictions / cautions by victims of domestic violence	DPA	Police, legal & criminal justice	Victims of domestic violence who are divorcing or separating from an abusive partner can get legal aid to help. To qualify the victim must provide evidence of a criminal conviction or caution. The process of applying to the court where the ex-partner was sentenced, or thepolice force which gave the caution,is set out on the MOJ website here: http://www.justice.gov.uk/private-family-matters-legal-aid/victims-domestic-violence

Access to solicitor's files while under a lien.	DPA	Police, legal & criminal justice	Can solicitors refuse to answer subject access requests because they can claim a lien over an individual's legal file? When a solicitor agrees to advise or act on behalf of a client, the individual enters into a contractual relationship known as a 'retainer'. If that contractual relationship is terminated and the solicitor's fees have not been paid, the solicitor can in most circumstances retain the file of papers until either the fees are paid or another satisfactory arrangement has been made eg an undertaking as to costs has been given by the client's new firm of solicitors. This is known as exercising a lien over the papers. In the situation where the client has not paid their bill and has asked for a copy of their legal file, solicitors often withhold the file until the fees are paid claiming their liens over the file. However, Section 27(5) of the DPA means that the Act takes precedence over this lien and a subject access request should be dealt with in the usual way. A solicitor will not be obliged to provide all information in the file for various reasons eg an exemption may apply, some information may not be personal data and some information may relate to other individuals. The wording of Section 27(5) is as follows: "Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information." Therefore, if the information is held in automated form or in files which are caught by the DPA then the Act takes precedence over the practice of withholding the information until the fees are settled. However, it is worth bearing in mind that subject access provides a right for the requester to see their own personal data rather than a right to see copies of documents that contain their personal data. In practice, the easiest way to provide the relevant information is to supply copies of original documents, however, the data controller is not obliged to do this. Consequently, it may be possible for the solicitor to accurately summarise the information contained in the personal data whilst still retaining the actual documents themselves, and this might enable the solicitor to still exercise an effective lien.

Appealing a DN (decision notice)	FOI	Government - central	A decision notice can be appealed to the First Tier Tribunal (Information Rights). Any appeals must be made within 28 calendar days of the decision notice being signed. Guidance for how to appeal is outlined on the Ministry of Justice website: http://www.justice.gov.uk/tribunals/general-regulatory-chamber/making-an-appeal If either party disagrees with the outcome of the Tribunal in relation to a point of law, they can then apply for leave to apple to the Upper Tribunal. Questions about the appeals process should be directed to the First Tier Tribunal themselves. Contact information can be found on the Ministry of Justice website: http://www.justice.gov.uk/contacts/hmcts/tribunals/grc There is no access to the First Tier Tribunal (Information Rights), without having first brought a complaint the ICO.
Automatic Number Plate Recognition (ANPR)	DPA	CCTV & optical surveillance	ANPR systems are capable of collecting significant amounts of information. Because of this, it's important to conduct a privacy impact assessment. The PIA should clearly justify the need for the system and demonstrate its use is:proportionate; andnecessary. Where a vehicle registration mark (VRM) is collected as part of an ANPR system, the ultimate purpose of which is to identify and take some action against a living individual (such as to serve them with a parking fine) the VRM will be personal data at the point of collection. This is because the data controller is likely to come into possession of further information which will allow them to identify either the driver or registered keeper of the vehicle, or both. This position has been confirmed by the Article 29 Working Party. Personal data collected through ANPR should be handled in line with the principles of the Data Protection Act, ensuring: appropriate signage informs individuals that ANPR is in use;databases are accurate and up to date;retention periods are minimal and consistent with the purpose for which the information was collected;data sharing agreements incorporate appropriate safeguards to ensure the information is kept secure. For further information on ANPR, see pages 25-26 of the data protection code of practice for surveillance cameras and personal information.

Basic DPA definitions - DC,DS,DP, Personal data	DPA	Other	Data Controller A data controller is defined in part I s.1 of the DPA as: 'A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed'. Section 4(4) of the DPA further states that: 'It shall be the duty of a data controller to comply with the Data Protection Act Principles in relation all personal data with respect to which he is the data controller' A data controller must be a 'legal person', i.e. a legal entity. This term not only comprises individuals but also organisations such as companies and other unincorporated bodies of persons and is the entity responsible for the processing of personal data in a given situation. Data Subject The definition of a 'data subject' is defined in part I s.1 of the DPA as: 'An individual who is the subject of any personal data' The DPA says that a data subject does not necessarily need to be a UK national or resident, but they must be a living individual (because of the definition of 'personal data'). Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects. Data Processor The definition of a 'data processor' is defined in part I s.1 of the DPA as: 'Any person (other than an employee of the data controller) who processes the data on behalf of the data controller'. Essentially, a data processor is a separate legal entity who processes data on behalf of a data controller. The DPA introduces specific obligations upon data controllers when the processing of personal data is carried

			out on their behalf by data processors (see Sch.1 part II (11) & (12). The data controller retains full responsibility for the actions of the data processor and so the definition of data controller has an impact on this context. Personal Data Personal Data is defined in part I s.1 of the Act as being: .'...data which relate to living individual who can be identified;from those data, orfrom those data and other information which is in the possession of, or is likely to come into possession of, the data controller'. This includes... 'any expression of opinion about the individual and any indication of the intentions of the data controller or any other person towards the individual'.
Biometrics in schools	DPA	Education	The Protection of Freedoms Act 2012 places controls on the use of biometric systems in schools, for example for cashless catering or borrowing library books. The provisions in the Act will take effect from 1 September 2013, and the Department for Education (DfE) has advised schools to start planning for this implementation date. The DfE has produced"guidance on the requirements of the Act.”
Body Worn Video (BWV)	DPA	CCTV & optical surveillance	Because of their ability to be mobile, BWV cameras are likely to be more intrusive than fixed CCTV style surveillance systems. A privacy impact assessment should consider whether a BWV camera is:proportionate;necessary; andwhether it addresses a pressing social need. The PIA should justify separately the need for visual and audio recording, considering that:continuous recording will require strong justification as it is likely to be excessive;audio recording coupled with visual recording is likely to be more privacy intrusive; andfurther justification will be required when recording in sensitive areas where there is a higher expectation for privacy. It is important that clear signage is visible on the clothing of the individual operating the BWV. This is necessary in order to satisfy the fair processing provisions in principle 1 of the DPA. System users should choose systems which will minimise intrusion. Such systems should have the ability to be switched on and off and to record visual and audio separately. Where both visual and audio recordings are processed, these should be considered as separate data streams

			and controlled as such. This will help ensure that the captured data is handled in line with the data protection principles. For further information on BWV, see pages 26-29 of the data protection code of practice for surveillance cameras and personal information.
CCTV in Classrooms	DPA	CCTV & optical surveillance	The Information Commissioner has received enquiries from individuals regarding CCTV in classrooms, and in particular, about an organisation called Classwatch. In essence Classwatch are marketing a technology; it is for schools to decide whether their use of such a system is proportionate and reasonable. Line to take The ICO advises that:Schools seeking guidance on this issue should consult our CCTV Code of Practice. This makes it clear that organisations will have to consider very carefully whether use of any surveillance system is necessary to address a pressing need, such as public saftey and crime prevention; whether it is proportionate to the problem it is designed to deal with, whether it is justified in the circumstances and whether people know it is going on.We recognise that CCTV surveillance is a sensitive issue, particular when children are involved. For that reason, schools should consult parents when making any decision to use such a system.

CCTV signage where there is a potential detriment to individuals by identifying the Data Controller	DPA	CCTV & optical surveillance	Background To be used in situations where identifying the organisation operating CCTV may cause potential detriment, for example outside a women's refuge or mental health care accommodation. Line to take We recognise the balance to be struck between the privacy rights of the individuals residing in these properties and those of the wider community. Where it is not obvious who is operating the system, and it is possible that providing the identity of the data controller on CCTV signage may have a detrimental effect on individuals who are residing at the premises, the DPA will not dictate that this information must be provided on a CCTV sign. In these circumstances a CCTV sign should provide people who would be captured by the equipment with the following information:That CCTV is in operation.The purpose of the CCTV if this is not obvious (ie on a building people will generally expect the purpose for the camera is crime prevention).A contact telephone number or address where an individual can write to exercise their rights under the DPA. If the information outlined above is provided then any individual captured by the CCTV cameras would be able to contact you to obtain the other fair processing information they may require to exercise their rights under the DPA.

Charging for public information.	FOI	Government - central	FOIA The FOIA allows the public authority to charge for providing information in a publication scheme (s19(2)). Any charges the public authority wishes to make should be included in the schedule of fees, and the basis for the charge should be made clear. Examples of charges public authorities may wish to make are:to cover costs of printing, copying or postagecharges under other statutory charging regimescharges for commercial publicationscharge for the reuse of a dataset (Statutory Instrument 2013 No. 1977) Any charges made must be reasonable and justifiable. EIR The EIR allows the public authority to charge a reasonable amount for providing environmental information in some circumstances (r8). Any charges the public authority wishes to make should be published, and the basis for the charge should be made clear. The EIR does not allow a charge to be made for access to public registers, lists of environmental information, or examining the information in-situ.
CLI identification	PECR	Internet & technology	Regulation 10 of the PECR talks about the provider of a public electronic communications service providing users with a simple means of preventing presentation of their number when they make a call. PECR is silent on what happens when the receiver of the call reveals the withheld telephone number. However we may be able to look at a concern about this under the DPA and in particular the first principle.

Cloud Computing and the US Patriot Act	DPA	Internet & technology	Some data controllers may be concerned about using a cloud provider/data processor in the USA due to the US Patriot Act. Line to take The Patriot Act allows US law enforcement agencies, such as the FBI, to take any information stored in the US away without the processor being allowed to disclose that fact to an EEA data controller. Clearly this is a risk that needs to be taken into account by any EEA based data controllers when they are looking to outsource their processing operations or seek a cloud provider with processing operations in the US. However it is not up to the ICO to make the decision on behalf of UK data controllers whether or not to choose processors in the US. We have already said as much in other guidance we have issued. The following example may give data controller some reassurance and clarity on what we would do in certain circumstances once such an action by the processor to disclosure a data controller's data to a US law enforcement agency comes to our attention (this is taken from our cloud computing guidance): If a cloud provider was required to comply with a request for information from a foreign law enforcement agency, and did so, the Information Commissioner would take the view that the cloud provider will be the data controller in respect of that disclosure rather than the cloud customer. This is because the cloud provider made the decision to disclose based on a legal obligation it was under, regardless of the cloud customer's wishes. Regulatory action against the cloud customer would be unlikely so long as they made a proper assessment taking into account the powers of law enforcement agencies and others to access the data in the jurisdictions where the cloud provider in located. If the powers of the law enforcement agencies or others are comparable to those of similar organisations in the EEA then they are unlikely to render the level of protection inadequate. Regulatory action against a cloud provider, in its role as a data controller, is unlikely provided it is responding to a request it is legally obliged to comply with. All you need to do is substitute "cloud provider" for "data processor" and "cloud customer" for "original / client data controller" to make the guidance more general.

			[Above supplied by Ian Williams, SL, 20/06/12]

Community CCTV schemes (access to footage)	DPA	CCTV & optical surveillance	Background We sometimes receive requests for advice from housing organisations regarding the operation of CCTV systems where the footage is accessible to residents (usually through being streamed to monitors within individual flats). Line to take •Advise that the ICO cannot give formal approval to such a scheme. It is for the housing organisation, as the data controller, to decide whether it is possible to introduce such a scheme in compliance with the Data Protection Act. •The housing organisation, as the data controller, would need to be clear about the purpose of the proposed scheme. They would need to determine whether such a system is justified, taking into account what benefits could be gained and consider overall whether this would be the most appropriate way to be dealing with the security of the housing and the prevention of crime. •They should consider the level of impact it is likely to have on people's privacy; and how such a scheme would operate in practice – in particular, how they would comply with the DPA's principles. •If residents had access to the footage then our main concerns would be the fact that residents could potentially view distressing footage if there was no authorised person viewing the footage to enable the system to be shut down when required. We would also be concerned if the residents have the facility to record any images they view.

Companies in administration	DPA	Other	If the company entering administration is a data controller in its own right, the administrator simply acts as a new chief executive, with the company still as the data controller; that is, the administrator will be making the decisions as part of the company. (This is the case until the administration process is complete.) If the company that enters administration is acting as a data processor, then the data controller(s) still have legal liability for the personal data being processed on their behalf ie any legal responsibility the data processor has to safeguard personal data will result from the contract it has with the data controller(s) and the administrator would need to honour this. If the data processor can continue to operate while in administration with a realistic prospect of the business being rescued, then the data protection concerns should be minimal but any data controller(s) would need to monitor the situation for any changes and may wish to put in place a long term succession plan. If the data processor is going to be dissolved by the administrator, then clearly the data controllers need to have a plan in place to deal with the personal data being processed on their behalf. If data controllers are experiencing problems with the administrator, then The Insolvency Service may be able to help them. Can the ICO take action against a company that has gone into administration? If a data controller is in administration, it is likely that the ICO would not be able to identify whether or not a breach of the DPA has occurred. Even if we could establish that there had been a breach, there would be no active organisation to take the required remedial action. In legal terms, once that legal entity has ceased to exist, then there is no data controller in terms of the DPA. So there is no further action that the Information Commissioner's Office can take.
Cookie Directive - New powers and obligations	PECR	Internet & technology	The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 – SI 2011 No. 1208 have come into force on 26 May 2011, amending the Privacy and Electronic Communications Regulations 2003. It isthe UK enactment of Directive 2009/136/EC – known as the EU Cookie Directive. New amendments include:new obligations for some organisations to notify the Commissioner, and in certain circumstances, the data subject, where security breaches occur;a power for the Commissioner to audit certain organisations in respect of their security breach reporting obligations;increased powers for the ICO to punish organisations – including a power to fine up to £500,000;a power to serve 'Information Notices' on certain third party organisations, asking for information to help us identify organisations which are breaching the

			PECR. Security obligations and reporting personal data breaches. What are the new obligations?An increased obligation to keep public electronic communications services secure; andObligations relating to reporting 'personal data breaches'. Who do these new security obligations apply to? Providers of a 'public electronic communications service' – for example, internet service providers and telecommunications providers. What are the new security obligations? The minimum possible is taking appropriate technical and organisational measures to safeguard the security of that service. Regulation 5(1A) sets out the minimum security measures for providers of public electronic communications services:that personal data can only be accessed by authorised personnel for authorised purposes;that steps are taken to protect that personal data; andthat a security policy is in place to protect that personal data. What is the Commissioner's new PECR audit power? This is a very narrow power to audit certain organisations' compliance with:the security obligations set out in Regulations 5(1) and 5(1A); andthe security breach reporting obligations set out in Regulation 5A. Put simply, the Commissioner can audit the security measures taken to protect the public electronic communications service and if breaches have been appropriately reported. Who can the Commissioner audit under this new power? Providers of a 'public electronic communications service'. What are the new security breach reporting obligations? Regulation 5A states that providers of a public electronic communications service must:report a 'personal data breach' to the Commissioner; andwhere a 'personal data breach' is likely to adversely affect the personal data or privacy of a subscriber/user, notify that subscriber/user of that breach too. The information which must be shared in each situation is set out in Regulations 5A(4) and (5). What is a 'personal data breach'? A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service. What if an organisation does not report a personal data breach? Regulation 5C introduces a new fixed monetary penalty of £1,000 for the Commissioner to use. This can only be used where the ICO becomes aware that a provider of a public electronic communications service has failed to report a data security breach to the ICO.

CRA Arrangements to pay - fairness of then registering a default	DPA	Finance	As stated in the old default guidance, where an arrangement to pay breaks down, a default may be filed when the total value of the arrears is equivalent to three monthly payments under the original terms. However, this should not result in the customer being placed in a worse position than someone who had made no effort to pay whatsoever. Whether an individual has been left in a worse position or not is something that we will have to consider on a case by case basis. However where we feel that the arrangement to pay has left the individual in a worse position than someone who simply stopped paying, we would normally consider this to be unfair under the first principle and ask the lender to amend the default so that it was the same as if the individual had simply stopped making payments without entering the arrangement to pay.
CRA Can I stop them from processing my personal data?	DPA	Finance	If the records are accurate, there is no right of deletion under the Data Protection Act and therefore, the ICO could not compel the credit reference agencies to delete any individual's personal data. Section 14 of the Data Protection Act 1998 gives individuals the right to ask for the records to be amended or deleted only if they are inaccurate and they would need to do this through the courts rather than the ICO. Section 10 of the Data Protection Act provides a more limited right for individuals to request an organisation to cease processing their personal data if it is causing or is likely to cause them substantial damage or substantial distress that is unwarranted. However, it appears unlikely that an individual would be able to show that the processing of accurate data by a credit reference agency was causing them substantial unwarranted damage or distress.
CRA Default on a credit file Vs default under the CCA	DPA	Finance	I was not sent any default notices, should the default on my credit reference file be removed? In most cases, the answer will be 'no', provided that adequate fair processing information was provided when the account was originally opened. It may help to explain that a "default" on an individual's credit file does not mean that an individual has been defaulted under the Consumer Credit Act; essentially, the same word is being used to describe two slightly different things (which can obviously lead to some confusion). Instead, a "default" on a credit file simply means the lender considers the relationship between itself and the individual to have broken down. Therefore, whilst it may be a requirement of the Consumer Credit Act to issue default notices, there is no DPA obligation on a lender to issue a default notice to individuals before marking an account as being in default on their credit file. Although we advise that it is good practice to issue a notice, lenders will often have provided individuals with fair processing information about defaults and notices in the terms and conditions when the

			account was opened. Provided this was the case, then it is likely to satisfy the “fairness” aspects of the first principle.
CRA Defaults - Guidance for filing defaults	DPA	Finance	Updated guidance for filing defaults with credit reference agencies was published on 1 January 2014. The official site can be accessed athttp://www.scoronline.co.uk/key_documents/ and the relevant document is entitledPrinciples for the Reporting of Arrears, Arrangements and Defaults at Credit Reference Agencies This is not the ICO’s guidance but a new document drawn up by the credit industry in consultation with the ICO which is now intended to be the main source of information for the public on this topic. This may create some impact on calls to the Helpline or complaints received where an individual is concerned that a default has been registered incorrectly on their credit reference file. Although the new guidance does not cover this in any depth, it is important to make individuals aware that there is a difference between a ‘default notice’ and a ‘default’ registered on a credit reference file. A ‘default notice’ is a communication a lender should usually send to a borrower before defaulting a credit agreement regulated by the Consumer Credit Act (CCA).There is not necessarily any DPA obligation on a lender to issue a default notice to individuals. Although we advise that it is good practice to issue a notice, lenders often provide individuals with fair processing information about defaults and notices in the terms and conditions when the account is opened. If this is the case then this is likely to satisfy the “fair” aspect of the First Principle. The term ‘default’ on credit reference files is used to refer to the situation when the relationship between lender and borrower has broken down, and this scenario is explored in more detail in the updated guidance on defaults. So essentially, the absence of a formal ‘default notice’ would not prevent a default from being registered on

			an individual's credit reference file.If there are outstanding payments or arrears in respect of a loan or other account then an organisation would be within its rights to record thisat the credit reference agencies.Providingthe information recorded is an accurate reflection of events then the Fourth Principle would not be contravened.
CRA Defaults - Necessity of recording of defaults with multiple CRAs.	DPA	Finance	There is no requirement in the DPA for lenders to report details to all of the Credit Reference Agencies (CRA). There isn't a requirement in the DPA for them to report any information to the CRA's. However, it won't be a breach of the DPA for lenders to report the information to the CRA's as itwill be in their legitimate interests and the legitimate interests of other lenders to help them make responsible lending decisions. It is up to the lender to decide which CRA or CRA's they use (if they decide to use one).

CRA Defaults - Recording of defaults relating to debts that have been sold.	DPA	Finance	The practice of selling/buying debts is widely used. As long as the information is correctly recorded on a credit file by the lender selling the debt and the lender buying the debt, then two entries relating to one account would not be considered to be a breach of the Data Protection Act provided that:-both recorded entries are shown as being in relation to the same account/debt; the original debt entry should be shown on the credit file as being either 'settled' or 'zero' balance and should show that the debt has been 're-assigned'; the new DC who shows the debt in their name should maintain the original default date and the correct balances; the retention period for maintaining the information on a credit file should be based on the original default date regardless of who is responsible for the entry/debt.
CRA Defaults - Showing defaults relating to unenforceable debts.	DPA	Finance	The ICO has considered the circumstances in which the credit reference agencies should be permitted to record details of unenforceable credit agreements. In doing so we have had particular regard not only to the clear legislative intent that the absence of a signature on a credit agreement should no longer be an absolute bar to enforcement, but also to the following factors; 1.The question of whether a legal liability exists in relation to a credit agreement is quite separate from the question of whether such a liability may be enforced by the creditor. 2.Where a liability does exist, creditors have a legitimate interest in sharing relevant information about that liability, including information about whether the amount due has been repaid. Such information may properly inform responsible lending decisions, regardless of whether the liability is enforceable. 3.Responsible lending decisions are dependent upon lenders receiving accurate information about individuals' ability (and/or inclination) to repay their debts. Where a credit agreement clearly existed and credit has been provided to the debtor, but the debtor is not obliged to repay the loan due to the provisions of the Consumer Credit Acts, this does not mean that there was no agreement in the first place. It simply means that there was no enforceable regulated agreement. It follows that, where the existence of the agreement is not in doubt, we consider it to be appropriate for information about the agreement, including any failure by the debtor to repay his or her debt, to be recorded with the credit reference agencies. Where a 'debtor' disputes the existence of any credit agreement, enforceable or otherwise, we would ask to see evidence of the agreement and of its terms. This might include evidence of the provision of the credit facility or of a history of payments made by the debtor.

CRA Do they require consent to process personal data?	DPA	Finance	No. One of the conditions for processing in Schedule 2 is that the individual has given their consent to the processing. However another is that it is in the legitimate interests of a data controller. No one condition carries greater weight than any other. All the conditions provide an equally valid basis for processing. Examples. A company employs a debt collection agency to pursue a debt on their behalf. If the company (the data controller) uses a debt collection agency (the data processor) to pursue the debt on their behalf, then they wouldn'trequire the consent of the individual to do this. This is because the debt collection agency is acting on their behalf. This is the same as any other data controller data processor relationship where there should be a contact in place between them which explains what the data processor is allowed to do with the personal data. The data controller still has to ensure that the DPA is compiled with. A company sells the debt onto a debt collection agency. This is because the company that sold the debt on has alegitimate interest to reclaim any monies owed to them. In the majority of cases companies will also explain in their terms and conditions that this is a possibility if an individualisn't ableto make repayments. The company that debt has been sold onto will also then have a legitimate purpose to pursue the debt with the individual for monies that are outstanding.
CRA How accounts included in a bankruptcy should be recorded	DPA	Finance	Default date MUST be NO LATER than the date of the Bankruptcy. Settlement date (where shown) MUST be NO LATER than the date of Discharge.

CRA How payments on a debt management plan should be recorded	DPA	Finance	Payments on a debt management plan can be recorded in several ways, including, marking the debt with 'debt management program in force' or DF – account in default, or recording this fact in a notice of correction. All of the above can be correct, depending on the situation. Essentially, it depends on whether the lender is satisfied with the reduced payment that it is being offered. The following is based on the information in the old defaults guidance: Moderate to high levels of repayment – if the payment set out in the debt management plan (DMP) is at a level that a lender considers at least adequate, the agreement should be marked as included in a DMP. A lender may be willing to reschedule the agreement at a later stage (i.e. end the old agreement and start a new one under the new terms) at which point the record should be changed to reflect the agreed rescheduling. Low repayment levels – If the payment set out in the DMP is at a level that represents only a token sum in repayment because it is all the customer can afford, the account should be recorded as a default. A notice of correction can be added to the credit file by the customer, or the third party debt adviser acting on their behalf, to record the existence of the DMP. This will distinguish the customer from those who have acted less responsibly. The lender should bring the notice of correction facility to the attention of the customer and their debt advisers. In summary, marking the account as "debt management program in force" or similar means the lender is satisfied that the reduced repayment offered is adequate. Marking the account as defaulted means the lender does not consider the reduced repayment that has been offered to be acceptable. It should be noted that accepting a token payment does not mean the lender is considered to have accepted the amount as satisfactory. The lender can take such token payments (as the only realistic means of reclaiming any of the money it is owed) and still file a default. However, the lender should take particular care to ensure that the individual and/or debt adviser is made aware that this will happen and is not led to believe that the reduced payment constitutes a satisfactory reduced payment if this is not the case. Ultimately, from a data protection perspective, it is up to the lender to decide whether an offer of reduced payment is satisfactory or not. Organisations like the FCA or the FOS may be able to look into whether the lender has generally treated the customer fairly, but this isn't something we could get involved in. It is worth noting that we are currently discussing this particular issue with the industry. This particular line

			may therefore need updating in the future. In the meantime, it would be useful if First Contact can make Strategic Liaison aware of any complaints about this so that we have some examples to discuss with stakeholders.

CRA None credit organisations passing information to a CRA?	DPA	Finance	The telecoms and utilities sectors are not subject to the CCA. The following sets out the ICO's view on utilities companies sharing information with the credit reference agencies. Credit agreements are included on the credit file as well as other agreements such as telephone agreements, energy and water payments. The ICO has accepted that agreements such as utilities bills can be recorded on the credit file as in most cases the services are provided before they are paid for. There are exceptions, such as pre-payment meters, that should be handled differently. The water companies use the legitimate interests condition to share data with CRAs. However, they must be clear and transparent with consumers about what they are doing with the data and the data must be accurate. Sharing utilities data is a topic that consumer groups have focused on and they recognise that sharing utilities data should not cause unnecessary damage or distress to consumers. Clearly, accuracy problems resulting in the incorrect placing of a default on a credit reference file must be avoided. The Consumer Focus (now known as Consumer Futures) document below may be useful. It highlights the consumer benefits of utilities data sharing. http://www.consumerfocus.org.uk/files/2011/10/Consumer-Focus-On-the-record.pdf To conclude, as an office we have accepted that utility companies can pass personal data relating to outstanding payments to CRA's as explained above. However, even though we accept that this type of activity is allowed under the DPA, we are of course still concerned with other DPA related issues such as fairness (eg the adequacy of fair processing given to data subjects about potential disclosure to the CRAs), accuracy and the length of time the personal data are held. Therefore, if individuals believe that there are accuracy, retention or first principle concerns, they may still request an assessment of their case under Section 42 of the DPA. Rental Exchange This scheme involves local councils or Housing Associations providing information to CRAs. It is a project that is designed to help individuals improve credit ratings by having their rental payments included in the credit file. We have stated that just because Experian has informed us of the development of the project does not mean we endorse it in any way.

			Councils or Housing Associations need to make their own decision about entering into the project. It will be their responsibility to ensure that any project is correctly implemented fully addressing all the possible issues. We contributed the below to an Experian leaflet that sets out our position. "The ICO was approached about Rental Exchange in October 2010 and has had the opportunity to comment on data protection and privacy issues throughout the development of the project. It is anticipated that many of the housing associations considering using Rental Exchange will have similar queries relating to the Data Protection Act 1998 (DPA). For this reason, the ICO has addressed some of the common issues here. This is not an ICO endorsement of the Rental Exchange Project, it is a reflection of the advice that the ICO has provided to Rental Exchange and Experian since October 2010. Much of the discussion has focussed on the justification for sharing tenant's rental payment information. Above all else, data sharing must be fair, as well as satisfying the relevant conditions for processing. One such condition is consent, but gaining consent from data subjects is one of several other equality valid conditions for processing available under the DPA. The ICO is aware that the legitimate interest condition is being used in the context of Rental Exchange and the justification for this is explained by Experian above. Despite the use of the legitimate interest condition, the ICO is pleased to note that if a data subject does not want their data to be shared through Rental Exchange (having weighed up the benefits), their objection will be respected. This enhances the data subject's control over the use of their data and the general fairness of the project. The ICO is satisfied that discussions over the project reflect Big Issue Invest and Experian's understanding that a critical part of fulfilling the requirements of the legitimate interests condition is to be absolutely transparent with tenants about how their data will be used. The Fair Processing Notice has been developed by Experian and Big Issue Invest and the ICO's comments have been taken into account and incorporated into the final draft. Any housing association that previously informed existing tenants that their data will not be shared with CRAs or similar third parties should consider this when moving to Rental Exchange. This point was raised during discussions but it was considered unlikely to be relevant in most cases. Nonetheless, it should be considered by housing associations that are considering processing existing tenant's data in new ways. In addition to discussions about Rental Exchange, Experian has provided the ICO with updates on the project at regular liaison meetings. The ICO looks forward to continuing discussions as the project develops."

CRA Rapid updates and P4	DPA	Finance	It is our understanding that all three main CRAs offer a rapid update facility. The facility is, as described on the Experian website,"..a manual overnight update intended only for correcting significant errors that might, for example, prevent someone getting a loan. It is like a triage system in A&E to make sure the most serious cases are dealt with quickly." We do not interpret the ability to provide a rapid update in certain circumstances as a general obligation (under the "where necessary, kept up to date" provision) to provide one upon request, as long as the data controller has a reasonable updating procedure already in place, which we understand the main CRAs have at present. Internal line only- However, there may be individual examples where a rapid update is warranted and any refusal to do so when asked may be a breach of the fourth principle.
DBS checks and filtering	DPA	Police, legal & criminal justice	Information on DBS checks, including different types and what will appear on the check via Merideo link: Information on DBS checks, including different types and what will appear on the check Changes to the Disclosure and Barring service - filtering model Please note that as of 2 June 2013 a new filtering mechanism has been introduced which will mean, in many cases, old and minor offences will not be included on criminal records certificates issued by the DBA. There is filtering guidance on the government website:DBS filtering guidance. New filtering rules - For those 18 or over at the time of the offence: An adult conviction will be removed from a DBS criminal record certificate if: 11 years have elapsed since the date of conviction; andit is the person's only offence, andit did not result in a custodial sentence. Even then, it will only be removed if it does not appear on the list of offences relevant to safeguarding. If a person has more than one offence, then details of all their convictions will always be included. An adult caution will be removed after 6 years have elapsed since the date of the caution – and if it does not

			appear on the list of offences relevant to safeguarding. For those under 18 at the time of the offence:The same rules apply as for adult convictions, except that the elapsed time period is 5.5 yearsThe same rules apply as for adult cautions, except that the elapsed time period is 2 years. How would a Fixed Penalty Notice (FPN) or a Penalty Notice for Disorder (PND) be recorded on a DBS disclosure? Fixed penalty notices are generally used for anti-social behaviour such as parking illegally or some other driving related incidents. Accepting a FPN is not the same as admitting guilt for an offence as is the case when individuals accept a caution. Therefore, unlike cautions/reprimands, FPNs can be issued despite an individual's view of their innocence. The same is also true of Penalty Notices for Disorder (PND). Fixed penalty notices are not deemed convictions and so do not appear in the conviction part of the DBS Disclosure. However, if the Chief Constable believes that the behaviour giving rise to the issue of an FPN or PND is deemed relevant, then it may be disclosed in the 'Other Relevant Information' section of an enhanced criminal record disclosure but the mere fact that a FPN or PND has been issued would not be. In terms of the retention of fixed penalty notices on the police national computer, under the current rules, they will be held for 100 years. However it should be noted that this may change once the Tribunal has been completed in relation to the retention of conviction information on the police national computer.
Debt Collectors	DPA	Finance	Sometimes debt collectors will be acting as data controllers (for example, if they have purchased a debt from another organisation) and in other cases, they will be acting as data processors, acting on behalf of the organisation. Consent to pass personal information to a debt collection company would not be required because the company could rely on the legitimate interest condition to disclose this data. The Credit Services Association (CSA) has a Code of Practice –http://www.csa-uk.com/page/codes-and-standardsin regard to debt collection activities and how organisations which are members with the CSA should conduct themselves. If the debt collector is not actually seeking payment from the consumer, the Financial Ombudsman Service cannot generally consider a complaint from that person. So, for example, a consumer who simply receives a letter or telephone call from a debt collector intended for a previous resident at their address cannot normally complain to the FOS about receiving the communication. Whilst organisations may legitimately attempt to ‘trace’ individuals in order to recover monies owed, a ‘mis-

			trace' occurs when their search results in the subject of their tracing being mistaken for an individual with the same or similar name. Individuals who are concerned that they have been wrongly associated with a third party due to a 'mis-trace' should initially be advised to respond to the organisation(s) contacting them in writing and inform them that they are not the person being sought. The Credit Services Association has produced a FAQ on their website relating to mis-tracing which can be accessed from the following link:- http://www.csa-uk.com/assets/documents/factsheets/trace_factsheet_2014.pdf
Deceased Individuals - Information about.	DPA	Other	Background We receive a number of enquiries from people wishing to access information about deceased individuals Line to take Whilst the Data Protection Act 1998 gives certain rights to individuals regarding their personal data, the Act only applies to personal data relating to living individuals. Section 1 of the DPA states that: Personal data means data which relate to a living individual who can be identified from those data….. Therefore, if the records you are attempting to obtain relate to a deceased individual, the Act would not oblige the data controller to supply the data to you. However, you may have a right to access a deceased person's data from a public authority through the Freedom of Information Act. **Please note:** If a valid subject access request has been made by the deceased individual before their death, then there is a separate line for this.
Domestic CCTV	DPA	CCTV & optical surveillance	As CCTV and surveillance equipment becomes more readily available the Commissioner receives more and more calls relating to it's use by 'private' individuals. The most common complaint is the apparent monitoring of one resident in a street by another, usually in a neighbouring property. Line to take Key PointsIn these situations the Act is unlikely to apply due to section 36, the 'domestic purposes exemption'.Section 36 states that:

			‘personal data processed by an individual only for the purposes of that individuals personal, family or household affairs (including recreational purposes are exempt from the data protection principles and the provisions of parts II and III’.As the monitoring of a residential property is clearly going to fall under the category of ‘personal, family’ or household purposes’ the Act will not apply. This would be the case even if the cameras were to stray beyond the boundaries of the residential property. The critical point is that the 'purpose' for which the cameras are in place is 'personal, family or household'. However, many complainants argue that the monitoring conducted by their neighbour cannot be for domestic purposes because they are the focus of it. It is important to remember that the focus of the camera is not the issue, it is the purposes of the monitoring and the fact that those doing the monitoring are not classed as a data controller (as defined in the Act) that ‘triggers’ the section 36 exemption.Individuals should be advised that although the DPA is unlikely to apply, other legislation in the area of 'anti-harassment' or 'anti-social behaviour' MAY do. and consequently they should seek their own independent legal advice.
DPA Definition - "Health record" vs "Accessible record"	DPA	Health	The DPA makes specific reference to the term 'Accessible Records' when defining the kind of information the public have access to under the Act. In principle, individuals have a right to be given a copy of personal data held as part of an accessible record. Section 68 of the Data Protection Act 1998 contains further definitions of what would constitute an accessible record, these can include health records, educational records, and other records held by public authorities. The Durant ruling regarding manual records has no bearing on ‘accessible records’. They are accessible whether manual or not. A 'health record' is defined in the 1998 Act as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. (See S69 of the DPA for the definition of 'health professional'.) The definition of a 'health record' could apply to material held on an X-ray or an MRI scan, for example. This means that when a subject access request is made, the information contained in such material must be supplied to the applicant within the fee structure set out in SI 2000 No 191 and SI 2001 No 3223.

DPA Exemptions - Niche and Miscellaneous	DPA	Other	**Other Exemptions** These exceptions do not currently have a LTT, if you find out anything that may be useful or can clarify their use please let us know. Manual data held by public authorities S33A Category 'e' data is exempt from all provisions of the DPA except principle 4, S7, S14, S13 in relation to S7 or S14, and enforcement. Category 'e' data which relates to employees of the public authority is exempt from all provisions of the DPA except enforcement. Parliamentary Privilege S35A Personal data is exempt from the first principle, (except the condition(s)), the second, third fourth and fifth principles, S7, S10 and S14, if the exemption is required for avoiding an infringement of the privileges of Parliament. Armed Forces Personal data is exempt from the subject information provisions to the extent which the application of those provisions would be likely to prejudice the combat effectiveness of the armed forces. Judicial appointments and honours Personal data processed for assessing a person's suitability for judicial office or the conferring of honours by the Crown is exempt from the subject information provisions. Crown Employment Personal data may be exempted from the subject information provisions by order where it has been processed for assessing a person's suitability for employment by the crown or for a ministerial appointment. Management Forecasting Personal data processed for management forecasting and planning during the conduct of business are exempt from the subject information provisions to the extent which the application of those provisions would be likely to prejudice the conduct of that business. Corporate Finance Where personal data is processed for the purposes of a corporate finance service provided by a relevant person, then the data is exempt from the subject information provisions to the extent which the application of those provisions would affect the price of any instruments, or where the exemption is required to safeguard an important economic or financial interest of the UK.

			Negotiations Personal data which consist of records of the intentions of the data controller in relation to negotiations with the data subject are exempt from the subject information provisions to the extent which the application of those provisions would be likely to prejudice those negotiations. Self-incrimination An organisation does not have to comply with a subject access request to the extent which compliance would reveal evidence of an offence, (other than one under the DPA), which he could be exposed to proceedings for. Information provided in response to a subject access request cannot be used against a data controller in proceedings brought under the DPA.
DPA Exemptions - Overview	DPA	Other	Most exemptions in the DPA exempt the data controller from complying with one or two sets of provisions set out in the Act (S27). The two sets of provisions are the 'subject information provisions' and the 'non-disclosure provisions'. The subject information provisions are:The fair processing requirement of the first principleThe right of subject access If the exemption exempts the data controller from the subject information provisions, then the data controller does not have to provide fair processing information or respond to subject access requests. Other than the exemptions in the DPA, there are no other exemptions which can apply to the subject information provisions, ie no other law can supersede these rights. The non-disclosure provisions are:The first principle, except the conditions for processingThe second, third, fourth and fifth principlesSection 10 (right to prevent processing likely to cause damage or distress)Section 14 (rectification, blocking, erasure and destruction) If the exemption exempts the data controller from the non-disclosure provisions, then the data controller does not have to comply with the provisions to the extent that they are inconsistent with the disclosure. Hence, an exemption from the non-disclosure provisions does not automatically exempt the data controller from complying with all of the provisions, only those inconsistent with a disclosure of personal data. Exemptions from the subject information provisions Section 29(1) – Crime and taxation (also exempts from other aspects of compliance with the first principle except conditions for processing)Section 30 – Health, education and social workSection 31 – regulatory activitySection 34 – publically available informationConfidential references given by the data controllerLegal Professional privilegeArmed forcesJudicial appointments and honoursCrown employmentManagement forecastsCorporate financeNegotiations

			Some exemptions provide an exemption from just the right of subject access, these are:Examination MarksExamination Scripts Exemptions from the non-disclosure provisionsSection 29(3) – Crime and taxationSection 34 – publically available informationSection 35 – disclosures required by law or made in connection with legal proceedings
DPA Exemptions - Section 28 – National Security	DPA	Government - central	This section provides an exemption from:the principles,individual's rights,notification,enforcement, andsection 55, where the exemption is required to safeguard national security. A Minister must certify that this exemption is required, and this certificate provides evidence that the exemption applies. Individuals have a right of appeal against this certificate to Information Tribunal, who may determine the certificate does not apply.

DPA Exemptions - Section 29 – Crime and taxation	DPA	Police, legal & criminal justice	Section 29(1) Section 29(1) provides an exemption from the first principle, (except the condition(s) for processing), and the right of subject access, to the extent that complying with the first principle or a subject request would be likely to prejudice any of the crime or taxation purposes. This means the exemption only applies to the personal data which would be likely to prejudice the purposes; it cannot be used as a blanket exemption for all personal data held, without consideration of the likelihood of prejudice. The DPA doesn't define 'likely to prejudice', but the ICO's view is that for the exemption to apply there would have to be a real and substantial chance that complying with the provision would damage one or more of the crime and taxation purposes. Section 29(2) Where personal data was originally processed for the crime and taxation purposes, but it is obtained by an organisation processing it for statutory functions, it is exempt from the subject information provisions to the same extent as any exemption applied under section 29(1). This means that if an organisation exempts some personal data under section 29(1), but this data is then passed on to a regulatory body, the regulatory body can apply the same exemptions that were applied under section 29(1) by the original organisation. Section 29(3) Section 29(3) provides an exemption from the 'non-disclosure provisions' for information processed for the 'crime and taxation purposes', to the extent that compliance with these provisions would be likely to prejudice any of these purposes. This means that if complying with any of the non-disclosure provisions would be likely to prejudice any of the crime and taxation provisions, then the organisation is exempt from complying from the applicable provisions. The exemption only applies to the non-disclosure provisions which would be likely to prejudice the purposes, so it is unlikely that personal data would be exempt from all the provisions even when section 29(3) is applicable. The DPA doesn't define 'likely to prejudice', but the ICO's view is that for the exemption to apply there would have to be a real and substantial chance that complying with the provision would damage one or more of the crime and taxation purposes. If an organisation is challenged on the application of section 29(3) they may need to defend their disclosure to the ICO or a court. Hence, any decision to apply the exemption must be justified and documented. It is up the organisation holding the personal data to determine when it would be appropriate to make a disclosure under section 29(3). There are no limitations on who can request disclosure from an organisation

			under this section, however as part of the organisation's decision whether to disclose, the identity of the requester should be a consideration. Section 29(3) is often referred to as a permissive exemption, as it enables an organisation to disclose information to a third party under certain circumstances, but it does not compel them to. As such, an organisation does not have to comply with any requests for disclosure they receive under section 29(3). Section 29(4) This section provides an exemption from subject access for personal data held by a public authority as part of a risk assessment relating to the crime and taxation purposes, where the offence involves an unlawful claim on public funds (ie fraud). The exemption applies to the extent it is required to protect the system.
DPA Exemptions - Section 30 - Health, education and social work	DPA	Health	Health The Data Protection (Subject Access Modification) (Health) Order 2000 (Statutory Instrument 2000 No. 413) provides an exemption for subject access for personal data processed in relation to health, where providing subject access would be likely to cause serious harm to the physical or mental health or condition of the requester or any other person. To apply this exemption there must be an assessment of the likelihood of the disclosure causing serious harm. If the data controller is not a health professional as defined in SI 2000/413 then the personal data should not be disclosed until a health professional has been consulted, or an exception applies. A further exemption from subject access to information about an individual's physical or mental health applies where a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party. The Data Protection (Subject Access Modification) (Health) Order 2000 Education The Data Protection (Subject Access Modification) (Education) Order 2000 (Statutory Instrument 2000 No. 414) provides an exemption for subject access, for personal data processed in relation to education, where providing subject access would be likely to cause serious harm to the physical or mental health or condition of the requester or any other person.

			A further exemption from subject access to education records applies when a SAR is made by a third party, where the personal data consists of information relating to child abuse, it is exempt to the extent that granting subject access would not be in the interests of the data subject. The Data Protection (Subject Access Modification) (Education) Order 2000 Social Work The Data Protection (Subject Access Modification) (Social Work) Order 2000 (Statutory Instrument 2000 No. 415) provides an exemption from subject access, for personal data processed in relation to social work, where providing subject access would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the requester or any other person. A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party. The Data Protection (Subject Access Modification) (Social Work) Order 2000
DPA Exemptions - Section 31 - Regulatory activity	DPA	Government - central	Personal data processed in connection with certain regulatory activity is exempt from the subject information provisions to the extent that compliance with the provisions would be likely to prejudice the regulatory activity. This exemption only applies to regulatory bodies whose function is one of the following: protecting the public against financial loss due to the actions of the financial services industry, or against improper conduct by businessesprotecting charitiesprotecting the health and safety of employees and members of the public The functions must be either; conferred by enactment, functions of the Crown or Government, or exercised in the public interest. This exemption applies to the public functions of several watchdogs, but it doesn't cover investigatory or complaint handling functions. It also only applies to the extent the complying with the subject information provisions would be likely to prejudice the regulatory activity, hence it is not a blanket exemption.

DPA Exemptions - Section 32 – Journalism, literature and art (the special purposes)	DPA	CCTV & optical surveillance	Section 32 relates to the personal data processed for the special purposes, which are defined in the DPA as journalism, literature and art. Personal data processed only for the special purposes are subject to this exemption only where the following three criteria are met:the processing of personal data is with a view to publication, andthere is the reasonable belief publication is in the public interest, andthere is the reasonable belief that compliancewith a provision is incompatible with the special purposes Section 32 provides an exemption from:the principles, except the seventhsection 7 (subject access)section 10 (right to prevent processing causing damage and distress)section 12 (rights in relation to automated decision making)section 14 (rectification, blocking, erasure and destruction) Section 32 also states that when an organisation is deciding if publication is in the public interest any relevant codes of practice should be considered. Section 32 does not provide an exemption from section 13; hence the individual could still claim compensation relating to a contravention of the DPA. Indeed, the only circumstance where an individual can make a claim for compensation relating to distress alone, (rather than damage and distress), is where the processing is for the special purposes.
DPA Exemptions - Section 33 - Research, history and statistics	DPA	Education	Section 33 provides an exemption for the processing of personal data which meets the 'relevant conditions':the processing is for research, historical or statistical purposes, andthe data is not used in a way which would affect any particular individuals, andit is not processed in a way which would cause substantial damage or distress to the data subject Section 33 provides an exemption from:the second principle (processing for research purposes should not be considered incompatible with the purposes it was obtained for)the fifth principle (personal data processed for research purposes may be kept indefinitely)the seventh principle, if the results are not made available in a form which identifies data subjects
DPA Exemptions - Section 34 - Information made available to the public by or under enactment	DPA	Government - central	If a data controller is obliged to make personal data publically available due to any other legislation, then the personal data is exempt from:the subject information provisionsthe fourth principle and section 14the non-disclosure provisions This exemption applies whether the personal data is made available for free, or only upon payment of a fee. Some of the more common examples of where section 34 applies are:The Companies Act 2006 – publication

			of personal data of company directorsTown and Country Planning Act 1990 – publication of personal data relating to individuals making planning applicationsPublication of names and addresses on the electoral registerCivil Procedure Rules – publication of court transcripts
DPA Exemptions - Section 35 - Disclosures required by law or made in connection with legal proceedings	DPA	Police, legal & criminal justice	Section 35(1) Section 35(1) provides an exemption from the non-disclosure provisions in circumstances where the disclosure is required by other legislation or a court order. If an organisation receives a court order to disclose information, or is required by other legislation to do so, then they are compelled to provide it, as not to do so would be an offence, or a breach of the legislation concerned. As such, this is the only situation in which an organisation would be required to disclose third party personal data. Section 35(2) Section 35(2) provides an exemption from the non-disclosure provisions where the information is necessary for the purposes of (prospective) legal proceedings, obtaining legal advice, and otherwise upholding legal rights. The legal proceedings can be civil or criminal, this is not specified in the DPA. This exemption is permissive, which means that it allows an organisation to disclose a third parties personal data in certain circumstances without being in breach of the DPA, but it does not compel them to. An organisation is entitled not to respond to a request under section 35(2). If an organisation receives a request for third party personal data under section 35(2), they would need to consider whether disclosure of the information would meet the criteria outlined in the exemption. If they cannot assure themselves of this, then they may well decide not to release the information, as a disclosure may then be in breach of the Act. As organisations are not compelled to provide information under such an exemption, they may choose to be discretionary about when they do make a disclosure, eg to only provide information when it is requested by the police.

DPA Exemptions - Section 36 - Domestic purposes	DPA	Other	This exemption applies where information is processed by an individual, and it is processed only for the purposes of their own personal, family, household, or recreational affairs. Section 36 provides an almost total exemption from the DPA. It exempts individuals from complying with all of the principles, all individual's rights and notification. The only part of the DPA which still applies are the powers of the ICO, meaning the ICO could still investigate whether an individual had gone beyond the scope of the exemption.
DPA Section 10 - Right to prevent processing	DPA	Other	We can only look into a concern about section 10 if the organisation hasn't responded to the request within 21 calendar days.We can'tmake a decision on whether the organisation should comply with the request or not. The individual can apply to a court for a decision and the court can decide whether the request is justified. In more detail on section 10: Individuals have a right under section 10 of the DPA to request in writing that an organisation ceases processing their personal data if it is causing them, (or is likely to cause them), substantial and unwarranted damage or distress. However this right does not apply if any of the first four conditions of processing in schedule 2 are being used to process the personal data. These are:the individual has given their consent to the processing;the processing is necessary for the performance of a contract to which the individual is a party;the processing is necessary for compliance with a legal obligation; andit is necessary in order to protect the vital interests of the individual. The right may apply if the last two conditions of processing in schedule 2 are being used to process the personal data. These are:the administration of justice, exercise of Crown/Parliamentary functions and functions of a public nature; andfor the purposes of legitimate interests pursued by the data controller. How to make a request under section 10the request needs to be made in writing to the organisation;asking them to cease processing their personal data;explaining why the processing is causing unwarranted and substantial damage and distress. What the organisation needs to dothe organisation needs to determine whether or not the request is valid in line with the above points;make an assessment whether there is damage and distress being caused by the processing; andrespond to a valid request within 21 days to explain whether they are going to comply in full, part or not at all. What a data subject can do if the organisation refuses to comply with a requestthey can apply to court for them to determine whether the request is justified;if the court decides it is, they can then order the

			organisation to comply; andthe only situation where the ICO can get involved with a request made under section 10 is where the organisation hasn't provided any response within 21 days, we cannot assist with any matters relating to compliance with the request.
DPA Section 55 - Business to business	DPA	Employment	Note-- Please only use this letter in specific circumstances, it is not a general sctn 55 letter. Before using, please first check with a manager or LCO Copy this text into a CMEH generated letter: In the first instance I should make it clear that the main purpose of the Data Protection Act 1998 ('the Act') is to protect the rights of individuals in respect of personal information which relates to them, not to protect the commercial interests of businesses or companies who hold that information. With this in mind, whilst I appreciate your concerns, I should make clear that it is not our policy to pursue 'business to business' matters where little or no detriment has been caused to those individuals to whom the information relates and who can be identified from that information, that is to say, individuals who are the subject and focus of the information. The Information Commissioner will consider detriment to have been caused in instances where loss or harm, or upset and aguish, over and above annoyance level, has been suffered by individuals who are the subject and focus of the information. On the basis of the information you have provided, it does not appear as though any individuals who are the subject and focus of the information have suffered detriment in this instance.

			The Information Commissioner is a publicly funded body and therefore must target his resources to appropriate areas. Further information outlining the Information Commissioner's policy on this matter is contained in our 'Strategy for Data Protection Regulatory Action', which can be located on our website atwww.ico.go.uk. We do stress that businesses should make it clear to all levels of staff what they can and cannot do with the personal data they use. To avoid confusion we would also suggest that businesses consider including post employment restrictive covenant clauses in employment contracts to clarify who controls the personal information and to set requirements as to what happens when employees go to work for another business. Businesses may always seek redress in the courts regarding such matters and any breach of a restrictive covenant clause would add weight to any such case. Further, please also note that in order to deliver compliance with the security provisions of the Data Protection Act 1998, organisations who process personal information should ensure that they have appropriate technical and organisational measures in place to safeguard against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information. As things stand, and for the reasons set out above, we do not intend to take any further action in this matter.
DPA Section 56 - Enforced Subject Access	DPA	Employment	**The implementation of this provision has been delayed. New information will be provided in due course.** The old guidance is as follows: S.56 DPA - Enforced Subject Access Section 56 of the DPA has never been commenced. If the provision was commenced it would be a mean a vital safeguard would be in place to prevent employers/potential employers circumventing the Rehabilitation of Offenders Act 1974 and the criminal records disclosure regime. Section 75 of the DPA provides that S56 of the DPA is commenced only once certain sections of the Police Act (S112) are commenced. This would be the introduction of basic checks which would mean employers would have an alternative route to obtain information about a potential employee as opposed to requiring individuals to make subject access requests. S112 is in force in Scotland and Northern Ireland but has not been commenced in England and Wales. Basic disclosures would provide a more privacy friendly and proportionate way of providing prospective employers with unspent conviction information or confirmation that there is no such information with important safeguards in place.

			We know many people are still being forced by their employers/potential employers to make a subject access request for their police records which circumvents the safeguards in the criminal record vetting check process. Forcing individuals to use their subject access rights in this way means that employers obtain more information (including spent convictions) than they would obtain if they were to go through the Disclosure and Barring Service (DBS) process. It should also be noted that those organisations requiring individuals to make subject access requests may not even be entitled to make those checks if they were made through the DBS (ie the individual not working with children or vulnerable adults). The police do refer cases to us where enforced subject access is suspected but given that the practice is not currently illegal there is little we can do.
Drones / Unmanned Aerial Systems (UAS)	DPA	CCTV & optical surveillance	UAS refers to the whole system under which unmanned aerial vehicles (UAV) operate – these are sometimes referred to as Remotely Piloted Aircraft Systems (RPAS) and Drones. Where a UAS is used for professional or commercial purposes, the data protection principles will apply. A privacy impact assessment should demonstrate strong justification for the use of UAS and privacy by design features should be incorporated into the devices. The PIA should justify the need for any recording and demonstrate that the recording is:proportionate; andnecessary. Special attention should be given to the need to provide fair processing when UAS are in operation. This is especially so because individuals are unlikely to realise they are being recorded. System users should choose devices which will minimise intrusion. Such devices should have the ability to be switched on and off and have mechanisms to facilitate and limit unnecessary recording. For further information on the use of UAS, see pages 29-31 of the data protection code of practice for surveillance cameras and personal information.

DVLA releasing keeper details - Protection of Freedoms info only.	DPA	Government - central	This guidance is only to be used in connection with concerns about the provision of vehicle licencing information by the DVLA outside the requirements of the POFA. Background Concern has been expressed that the DVLA may be acting in breach of the Data Protection Act 1998 (DPA) in situations where it provides a vehicle keeper's details to a parking operator if the operator is unable to comply with the provisions of Schedule 4 of the Protection of Freedoms Act 2012 (POFA) when seeking to claim payment of a parking charge from the vehicle's keeper. Provisions of the POFA Schedule 4 of the POFA prohibits private parking companies from requesting keeper details from the DVLA:- Until more than 28 days have elapsed following the issue of a manual ticket in respect of a vehicle infringing the terms and conditions of parking in a private car park; orAfter 14 days when the offending vehicle has been spotted using ANPR/CCTV in a private car park. Whilst the Schedule 4 provisions of the POFA are drafted to ensure that car park owners are required to seek payment of unpaid charges promptly, the period of 14 days for the car park owner using a camera system to contact DVLA, obtain keeper details and then issue a Notice to Keeper does appear to be unrealistically short in some cases. There is therefore potential for car park operators to use keeper details outside of the Schedule 4 provisions of the POFA and try to recover unpaid charges from vehicle keepers despite being unable to comply with the 14 day time limit imposed by the POFA. Is the DVLA making an unauthorised disclosure in breach of the DPA, if the disclose the keeper details outside the 14 day period? The fact that the 14 day period for service has not been (or in some cases, cannot be) complied with by the car park owner merely prevents the car park owner seeking repayment of the debt by serving a notice on the vehicle keeper. That the car park owner cannot enforce repayment does not remove the fact that the debt to the car park owner exists. In such circumstances the DVLA may find that the car park owner has '**reasonable cause'** for seeking the keeper's details (even if the owner cannot issue a Notice to Keeper) and therefore, in disclosing information to the operator, the DVLA has not made an unauthorised disclosure of personal data. That action cannot be taken by the operator in accordance with the POFA does not invalidate DVLA's basis for providing the keeper details as explained above.

			Conclusion It is government policy that reasonable cause is applicable in cases where there is some form of liability on the part of the vehicle user and the disclosure of keeper details to landlords or their agents to follow up alleged parking contraventions on private land is considered reasonable cause. Our view is that, under the existing legislation, DVLA has carried out its duty to check reasonable cause by insisting that the relevant parking companies are members of the British Parking Association (BPA) scheme. The BPA is then responsible for checking that participating companies adhere to its Code of Practice. DVLA has taken the view that the fundamental requirements for reasonable cause to be established to support the disclosure of vehicle keeper information have not been affected by the POFA provisions and we accept this view, although may review our stance if it were to become apparent that the provisions were being blatantly disregarded by some car park operators.
Elections	DPA	Political parties	**Definition of personal data:** S.11 (3) DPA defines marketing as: 'The communication (by whatever means) of any advertising or marketing material which is directed to the particular individuals.' The ICO takes a broad view of this definition to include the sale of goods or services and also the promotion of aims and ideals of an organisation including political parties. Our broad view was supported by the Information Tribunal in 2006 when it dismissed the Scottish National Party case who argued that political campaigning was not marketing. **Use of the Electoral Register by Political Parties:** Political Parties are entitled to use the full electoral register for electioneering purposes, there is no legal opt out from this. So this means that the use of the electoral register for this purpose is 'automatically fair' under schedule 1 part 2 (2). Also, this means that the Political Parties can use the electoral register to knock on people's doors and canvas. This is not an issue in relation to the DPA.

			However, they do have to comply with other parts of the DPA and PECR. A summary of these rules are set out below in relation to the type of marketing: **Marketing by post** Section 11 allows an individual to opt out of receiving marketing by writing to the organisation. The only exception to this is when a candidate in a parliamentary election sends an election address to an individual under s.91 of the Representation of the People's Act 1983. If leaflets are unaddressed or to the 'occupier' and delivered by the Royal Mail or volunteers these are not caught by the definition of marketing as they are not communications 'directed to particular individuals' **Live Telephone Calls** Political Parties can make live telephone calls promoting their party to individuals as long as the individuals are not registered on the Telephone Preference Service, have not previously asked for calls to stop (this is under Regulation 21 of PECR), or have not served a section 11 DPA notice on the Political Party. **Automated Telephone Calls** Political Parties need prior consent from individuals before making automated calls to them. This is under Regulation 19 PECR. **Email/SMS** Political Parties need prior consent from individuals before sending emails or texts messages to them. This is under Regulation 22 PECR. **Fax** Political Parties need prior consent from individuals before sending faxes to them. This is under Regulation 20 PECR. **In all Cases**

			The Political Party must identify them in the communication and provide contact details where the individual can opt out under section 11 DPA. **We have the following guidance on our website:** Guidance on political campaigning Data Protection Technical Guidance Note - Disclosures to Members of Parliament carrying out constituency casework Website - Political parties section **Political Party Enforcement Notices: Regulation 19: Automated Calls** Scottish National Party – 18 October 2005 Conservative Party – 18 October 2005 Liberal Democrats - 24 September 2008 Labour Party - 4 February 2010 **Requests for speakers** Please follow the usual procedure. Please do not get drawn into any conversations about whether it will be possible before the elections on 7 May 2015. The procedure can be found on ICON, but in the first instance take the details and email them to speakers@ico.org.uk **Any Sift items or HL calls about Political Party potential Breaches – national campaigns** Please let the LCO/managers know and they will escalate to the appropriate person. **'Purdah' for the Parliamentary elections on 7 May 2015.** The UK Parliament goes into 'Purdah' on 30 March 2015.

			'Purdah' means that the Parliament is dissolved and the elected members of the Parliament cease to represent their constituents. This means that they no longer have a right to personal data relating to their constituents as per our Technical Guidance Note: - Disclosures to Members of Parliament Carrying Out Constituency Casework. **Who is the data controller for the personal data the MP held before Purdah?** This is dealt with in advice to member's that the House of Commons produces. It says: **Section 6: Handling personal data during dissolution** **and when a Member leaves the House** **6.1 Handling personal data when Parliament is dissolved** 6.1.1 Members may continue to handle casework whilst Parliament is dissolved for all individuals who are content for this to happen. If there is any doubt, consent should be sought. **6.4 Reviewing records** A former Member will continue to be the data controller for all paper and electronic records that they hold and they must therefore be sure that anything they do with their records is in line with the expectations of the individuals concerned. For example, constituency casework records should not normally be passed on to a new Member or to a history centre/county archive unless the constituent is happy for this to happen. 6.4.2 Records relating to closed cases which are not likely to be reopened should usually be securely destroyed. 6.4.2 Live cases, and closed cases which are likely to be reopened, should be assessed on a case-by-case basis, considering the expectations of the

			individuals and consulting with them where their views are not clear. **Elections for local authority councils** Many of these also take place on 7 May 2015. Unlike MPs councillors remain in their role until they are either reelected or lose their seat. They have to follow all the DPA and PECR guidance. Councillors don't have a statutory instrument to allow them to act for their ward members without consent being requested. **The Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.** The next elections will be held on 5 May 2016 – more information will be available nearer the time.

Electoral Register	DPA	Government - local	Individual Electoral Registration Individual electoral registration was introduced in England and Wales in June 2014 and in Scotland in September 2014 following the Scottish Independence Referendum. It replaces the previous electoral arrangements - where one person in each household registered everyone to vote - with the requirement to register individually. People will also be able to register on line for the first time. For many people this change in how we register to vote will mean that they are now responsible for their own registration - including the choice on whether they wish to be included on the 'open' (edited) register. We explain this in more detail below. For general information on individual electoral registration and how to register, the Electoral Commission has information on its website athttp://www.aboutmyvote.co.uk/ Electoral registers are managed locally by electoral registration officers who, using information received from the public, keep two registers – the electoral register and the open (edited) register. What is the electoral register? The law makes it compulsory to provide information to an electoral registration officer for inclusion in the full register. The details you are likely to have to provide are your name, address, national insurance number, nationality and age. The full register is updated every month and published once a year, and is used by electoral registration officers across the country for purposes related to elections. Political parties, MPs and public libraries also have the full register. It is also used by local authorities for their duties relating to security, law enforcement and crime prevention, for example checking entitlement to council tax discount or housing benefit. It may also be used by the police for law enforcement purposes. It can be sold to government departments to help in their duties such as the prevention or detection of crime. They can also use it for vetting job applicants and employees if this is required by law. Credit reference agencies are allowed to buy the full version of the register so that lenders can check the names and addresses of people applying for credit and carry out identity checks to help stop money laundering. It is a crime for anyone who has a copy of the full register to pass information from this register onto others if

			they do not have a lawful reason to see it. What is the open (edited) register? The open register, also called the edited register, contains the same information as the full register but is not used for elections. It is updated and published once a year and can be sold to any person, organisation or company and used for any number of purposes. Users of the register include direct marketing firms and also online directory firms. It is not compulsory to have your personal details included in the open version of the register; however they will be included unless you ask for them to be removed. Removing your details from the open register will not affect your write to vote. Individual electoral registration means that for the first time many people may be making a choice whether or not they wish their personal details to be included in the open register. Some may also be unaware of the choices made on their behalf in the past. How can I opt out of the edited register? Some people may already be opted out of the open register - if you had opted out at the point of the last household electoral registration your preference will have been noted and carried forward with the introduction of individual electoral registration. If you are not already opted out but do not want your personal details on the electoral register made more widely available you can make a request at any time to your local authority electoral registration staff for your details to be removed. Your request needs to contain your full name and address and can be in writing, via email or phone. If you are registering online you can also indicate that you do not want your name and address listed on the open register. Under the individual electoral registration arrangements your preference as to whether your details are included in the open register will be carried forward – you will not need to make your choice annually when you receive your electoral registration form. It is important to understand that if you do not indicate you don't want your information to be made more widely available then, by default, the personal details you provide on the voter registration form will be included on both the full and open versions of the register. This means they will be made available to anyone who wants to buy the edited version.

			Additionally, those who believe that having their name and address on the electoral register would put them or anyone who lives with them at risk can apply for anonymous registration. Ask your electoral registration officer for further information. How can I update my details on the register? The updated electoral and open registers are published usually by 1 December. If you move house, you can re-register with your new address, and your new details will be included in the next monthly update of the full register. How can I opt out or update my details in Northern Ireland? From 1 December 2006, registration in Northern Ireland became continuous. This means that annual forms are not sent out to households. If you live in Northern Ireland and want to update your details or to notify that you do not want your details to be more widely available, it is up to you to submit the registration form, available from the Electoral Office for Northern Ireland. Why are my old details still available if I opted out? Prior to November 2001 the register could be sold to anyone prepared to pay a fee. A ruling by the High Court changed the law governing the use of personal information on the electoral register. The court confirmed that it was unlawful to sell copies of the electoral register to private businesses without giving people a choice not to have their information used in this way. It has come to our attention that some organisations which legitimately bought a copy of the register before the change in the law might still be using people's details contained in it. It is also possible that if an individual didn't opt out in each year since 2002, some organisations might also have their details in a version of the open register. Depending on the circumstances, the use by an organisation of an older version of the register may raise issues in relation to the processing of personal data, giving rise to a risk of a breach of the provisions of the Data Protection Act 1998. Such processing might be unfair and might not accord with the expectations of individuals.
Employer-funded pension or insurance schemes - sharing	DPA	Employment	Access to personal data arising from the administration of the scheme should be limited and information gathered in this context should not be used for any other purposes. When a worker joins a pension, health or insurance scheme, it should be made clear to them what, if any,

			information is passed between the scheme controller and the employer and how it will be used. An employer's funding of an insurance or pension scheme does not give the employer the right to receive information about individual members of the scheme unless this is necessary for the operation of the scheme, for example, to allow the employer to deduct contributions for pay or to decide whether to continue funding. Wherever possible, anonymised statistical information should be used. If medical information is shared between employer and insurer, a sensitive personal data condition must be satisfied.
Employers sharing personal data with unions	DPA	Employment	When can my employer share my personal data with the union? Personal information about workers should only be supplied to a trade union for its recruitment purposes if: • the trade union is recognised by the employer; • the information is limited to that necessary to enable a recruitment approach, and • each worker has been previously told that this will happen and has been given a clear opportunity to object. Where staffing information is supplied to trade unions in the course of collective bargaining, employers should ensure the information is such that individual workers cannot be identified. Aggregated or statistical information should suffice.
Employers using CCTV - summary	DPA	CCTV & optical surveillance	Some organisations may overtly monitor their staff with CCTV or other types of cameras. The Act would not specifically prohibit this type of monitoring as long as the eight principles are complied with, including, in particular, the first principle, ie that fair processing is provided to staff members, the processing is lawful, and a condition for processing is met. However, continuous video and/or audio monitoring is particularly intrusive for workers. The circumstances in which continuous monitoring of individual workers is justified are likely to be rare eg work in particularly hazardous environments such as refineries. This is different from the security monitoring of public or semi-public areas where workers may pass from time to time. Covert monitoring is when an organisation uses hidden cameras or other technology to record members of staff or individuals. Although the DPA would not necessarily prohibit this type of monitoring outright, it would only be justified in specific circumstances, where the intrusion is proportional to the reason for monitoring (eg a criminal offence is suspected). Even in circumstances where covert monitoring may be justified, a data controller should take steps to ensure that the monitoring is specific/targeted, proportional and only carried out for a limited

			period. It may be advisable to carry out a privacy impact assessment before taking the decision to carry out covert monitoring. If CCTV cameras are installed for crime prevention purposes but capture images of other staff activities, can this personal data be used for disciplinary purposes? Generally, personal data obtained for a particular purpose should not be used in a way that is incompatible with that purpose. It is likely to be unfair to workers to tell them that monitoring is undertaken for a particular purpose and then use it for another purpose that they have not been told about unless it is clearly in the worker's interest to do so or the information reveals activity that no employer could reasonably be expected to ignore. The type of activities that an employer could not be reasonably expected to ignore might include criminal activity at work, gross misconduct or breaches of health and safety rules that jeopardise other workers. Use of in-vehicle monitoring systems. Monitoring of vehicle movements, where the vehicle is allocated to a specific driver, and information about the performance of the vehicle can therefore be linked to a specific individual and will fall within the scope of the Data Protection Act. If an employer is considering introducing in-vehicle monitoring, they may wish to carry out a privacy impact assessment to ascertain whether the benefits justify the adverse impact. Key points to consider include:- • If the vehicle is for both private and business use, it ought to be possible to provide a 'privacy button' or similar arrangement to enable the monitoring to be disabled; • Where an employer is under a legal obligation to monitor the use of vehicles, even if used privately, for example by fitting a tachograph to a lorry, then the legal obligation will take precedence. Employers should establish a policy that states what private use can be made of vehicles provided by, or on behalf of, the employer, and any conditions attached to use. They should ensure that, either in the policy or separately, details of the nature and extent of monitoring are set out and workers using vehicles are aware of the policy.

Employers using gagging clauses relating to DPA, FOIA.	DPA	Employment	Occasionally, employers have asked employees to sign a compromise agreement containing some form of gagging clause preventing the employee from making any future FOIA or subject access requests. The ICO would take the view that even if such a compromise agreement has been signed, individuals may still exercise their rights to make requests under the Freedom of Information Act and/or Data Protection Act. If their employer refuses to deal with a request(s) because of the compromise agreement, they would be likely to be in breach of the above legislation. If this happens, the individual can complain to the ICO and request an assessment. However, individuals should be aware that if they exercise their information request rights there may be consequences such as legal action for breach of contract. The ICO cannot comment on whether any such "gagging" clause could be regarded as a fair contract term as contractual matters fall outside of our remit. Also, whether or not the clause would be a fair contract term would depend on the particular circumstances involved and the nature of the agreement signed. Clearly, individuals could seek independent legal advice to try and establish if this is a matter that they could take to Court; if a court found that the clause was not a fair contract term, it could not be enforced. **NB** The ICO could only make an assessment on a complaint where the individual has actually submitted an FOIA request or SAR after signing a compromise agreement and it has been refused. This is because neither the FOIA nor the DPA state that it would be a breach of these Acts if an organisation were to try and impose this type of contractual clause, and indeed, they do not address this issue at all. It would only be at the point where an individual made an information request and the organisation refused it (albeit on the basis of a gagging clause) that either Act could be breached.
Employers using information posted online	DPA	Employment	This line is specifically about complaints involving information which has been posted on a social networking profile or a blog and subsequently used by an employer in disciplinary action. In most cases the information comes to the employer's attention because the person posting it has an open profile, because they are friends with their manager, or because they are friends with a colleague who then brings it to the manager's attention. This line is applicable in situations where an individual has posted information which has been used against them. It should not be used in cases where an employer is actively monitoring staff activity online, either covertly or with staff knowledge. When dealing with enquiries on those issues you should refer to the employment practices code or seek further policy advice.

			Line to take It is important to note that in these circumstances the employer has not set out to obtain information using Facebook; rather, they have had information disclosed to them either by the employee or by a third party. It is very unlikely that an employer will be in breach of the DPA by having information disclosed to them. If an employer is made aware of information about an employee which they are entitled to act upon – for example, information which discloses possible misconduct – then the DPA will not prevent them from using that information just because it has been published on a social networking profile or in a similar online context. The issue at the heart of these complaints is generally whether any disciplinary action was a reasonable response to the circumstances confronting the employer. Primarily this is a question of fair employment practices, not fairness in DPA terms. Disciplinary action must be preceded by appropriate investigation and so employers should be wary of relying on information of dubious origin such as Facebook posts or hearsay. This is not a data protection issue: employees who have been unfairly dismissed or disciplined may make a claim to an employment tribunal. Callers should be directed towards the ACAS disciplinary code or other employment law advice if they are objecting to disciplinary action taken against them. The DP principles will apply when the employer is considering how to process any information they have been given. For example, if an employer continues to hold the information without taking disciplinary action, this processing might be unfair and excessive. Most questions about the continued processing of information in this context are covered by the employment practices code.

Employment reference - Provision without consent.	DPA	Employment	Employers should not provide confidential references about a worker unless they are sure that this is the worker's wish or unless they are under a legal obligation to do so. Clearly, an employer may regularly receive requests for information about individual workers from third parties. An employer has a responsibility to its workers to be cautious in responding to such requests. It risks a breach of the Act if it does not take sufficient care to ensure the interests of its workers are safeguarded. In some cases though, the employer will be able to respond positively to a request for disclosure if the circumstances of the disclosure are covered by one of the exemptions from the 'non-disclosure provisions" of the Act. Employers should be careful to only disclose information from sickness or injury records about an identifiable worker's illness, medical condition or injury where there is a legal obligation to do so, where it is necessary for legal proceedings or where the worker has given explicit consent to the disclosure.
Encryption of mobile devices	DPA	Internet & technology	ICO recommends that all laptop and other portable devices which contained personal information should be subject to some form of encryption. The following text has been produced following advice from a number of experts. The ICO recommends that all portable devices which hold personal information and removable media such as USB devices, PDAs, portable hard drives or any other form of memory storage that is not contained within the physical structure of the computer itself, which are used away from secure office accommodation should be protected by encryption software. Encryption software is designed to protect against the compromise of information by encrypting either the information held on the laptop or hard drive, or the complete hard drive itself, the latter by means of Whole Disk Encryption. There are a number of different options commercially available several of these products use variations or multiples of data encryption standards. Consideration should also be given to the use of specialised encryption products for PDA and USB devices. Encryption software uses a complex series of embedded mathematical algorithms to protect information. The information held on an encrypted drive is effectively hidden from any unauthorised individuals who do not possess the pass code or key to unlock the encryption algorithm.

			Since encryption standards are always evolving it is recommended that data controllers ensure that any solution that is selected meets the generally accepted standards in effect at the time.
Exam Marks and Scripts	DPA	Education	Examination marks (for any type of exam) are exempt from subject access where the request is made before the results are announced. The data controller must respond to the request within five months of the date of the request or within 40 days of the marks being released, whichever is sooner. Personal data consisting of information recorded by candidates during any type of exam are exempt from subject access. This does not include examiners comments.
Exemptions under FOIA / EIR and the PIT	FOI	Government - central	What is the difference between absolute and qualified exemptions? FOIA Absolute exemptions do not require a public interest test to be carried out, qualified exemptions do. Absolute exemptions are listed in s2. They are:S21 – information accessible to the applicant by other meansS23 – information supplied by, or relating to, bodies dealing with security mattersS32 – court recordsS34 – parliamentary privilegeS36 – prejudice to effective conduct of public affairs where the information is held by the House of Commons or LordsS40(1) – personal data of the requesterS40(2) + (3)(a)(i) – personal data where it would be a breach of the principles to disclose it,S40 + (3)(b) - where disclosure to the data subject under a SAR would be exemptS41 – information provided in confidenceS44 – information prohibited from disclosure EIR Exemptions are referred to as exceptions in the EIR. They are contained in r12(4) an 12(5). They are all subject to the public interest test. There are no exceptions which relate to personal data, this is covered in r13. What is the difference between class and prejudice based exemptions? FOIA Exemptions in the FOIA can be considered to the class based or prejudice based. Class based means that where the information is of the type described in the exemption, it is covered by that exemption. All absolute and some qualified exemptions are class based. Prejudice based means that the public authority has to satisfy itself that the prejudice or harm specified in the exemption would or would be likely to occur.

			The prejudice based exemptions are:S26 – defenceS27(1) – international relationsS28 – relations within the UKS29 – the economyS31 – law enforcementS33 – audit functionsS36 – public affairsS38 – health and safetyS43(2) – commercial interests These exemptions require determination of the likelihood of prejudice (the prejudice test). EIR The exceptions in r12(4) relate to the type of information or request (class based). Hence, if any of them apply to a request then the exception is engaged. The exceptions in r12(5) relate to situations where disclosing the information would have an adverse effect (prejudice based). Hence the exception is engaged when there would be an adverse effect on the interest listed in the exception. In the EIR, some exceptions refer to disclosures which would "adversely affect", rather than prejudice, various interests. Therefore, the prejudice test is referred to as the adverse effect test. What are the timescales for carrying out a public interest test? FOIA Where the public authority is required to carry out a public interest test, the timescale for compliance with the request can extended to a 'reasonable' time. This time must be justifiable, and the public authority must issue a refusal notice within 20 working days informing the requestor of the extension, and giving an estimated date by which it intends to reach a decision (s10). The 'reasonable' time is not defined in the FOIA, but in the view of the ICO the total time should not exceed 40 days. EIR There is no extension available in the EIR for considering the public interest. Requests should be handled within 20 working days, unless the public authority reasonably believes that the complexity and volume of the information makes it impracticable to comply within 20 days. In such circumstances the public authority can extend the period from 20 to 40 working days, but the requester must be informed of the extension within 20 working days (r7).
FOIA / EIR FAQs - Guidance docs Index	FOI	Government - central	Is an organisation covered by the FOIA/EIR? Public authorities under the Freedom of Information Act Outsourcing and freedom of information. Outsourcing and freedom of information What information is "held by" a public authority for the purposes of the FOIA/EIR? Determining whether information is held Information held by a public authority for the purposes of the FOIA

			Information held by a public authority for the purposes of the Environmental Information Regulations Determining whether information is held What is a valid request? Recognising a request made under the Freedom of Information Act (Section 8) Who can make a request? Consideration of requests without reference to the identity of the applicant or the reasons for the request What should the public authority do when they receive an unclear request? Interpreting a Request When should an EIR request be transferred? https://ico.org.uk/media/for-organisations/documents/1644/environmental_information_regulations_code_of_practice.pdf What information is covered by the EIR? What is Environmental information? What happens if information held by a public authority which is subject to a request is destroyed? Retention and destruction of requested information What is the cost/appropriate limit and when does it apply? FOIA Requests where the cost of compliance with a request exceeds the appropriate limit EIR Regulation 12(4)(b): Manifestly unreasonable requests What should the public authority do if the cost of compliance with a request exceeds the cost limit? Fees that may be charged when the cost of compliance exceeds the appropriate limit What is the time for compliance? Time limits for compliance under the FOIA Time limits for compliance EIR Can the means by which the information is communicated be specified? Means of Communication

			What are the provisions of the FOIA in relation to the format of datasets? Code of Practice (datasets) – external link to the MOJ website When can a request be deemed as vexatious under the FOIA? Dealing with vexatious requests Is there an equivalent of vexatious requests in the EIR? Regulation 12(4)(b): Manifestly unreasonable requests What if the public authority receives repeated requests about the same topic? Dealing with repeat requests When does the public authority need to offer advice and assistance? Good practice in providing advice and assistance EIR advice and assistance FAQs What happens if someone requests their own personal data under the FOIA/EIR? Section 40: personal information What happens if someone requests third party personal data under the FOIA/EIR? Section 40: personal information Section 40: information exempt from the subject access right Section 40: neither confirm nor deny in relation to personal data Section 40: personal data of both the requester and others What if a requester asks for information about public authority employees? Section 40: requests for personal data about public authority employees Can I make a request under the FOIA for information about deceased people? Information about the deceased Section 41: Information provided in confidence Regulation 12(5)(f): Interests of the person who provided the information to the public authority What are the grounds for refusing a request? Refusing a request under the EIR

			What must be in a refusal notice? Refusing a request: writing a refusal notice Refusing a request under the EIR What is the public interest test? The public interest test What are the timescales for carrying out a public interest test? FOIA Time for Compliance EIR Time for Compliance FAQs What is the difference between class and prejudice based exemptions? The prejudice test How exceptions and the public interest test work in the Environmental Information Regulations When does the commercial interests exemption apply? Section 43: commercial interest What is the procedure for internal review? Internal reviews under the EIR How does the ICO handle complaints under the FOIA/EIR? How we deal with complaints: a guide for public authorities Do we have to have a publication scheme? Model Publication Scheme What should be in the publication scheme? Model Publication Scheme Model Publication Scheme - Using the Definition Documents Definition Documents How much can we charge for information in our publication scheme? FOIA Charging for information in a publication scheme Charging for environmental information

FOIA requests to Academies	FOI	Education	All academies, by virtue of the Academies Act 2010, are subject to the Freedom of Information Act 2000. Department for Education guidance for academies on how they can comply with the Freedom of Information Act is available from the following link:- https://www.gov.uk/government/publications/academies-and-freedom-of-information/academies-and-freedom-of-information
FOIA timescales - requests to educational establishments	FOI	Education	For schools, the standard time limit for dealing with Freedom of Information requests is 20 school days, or 60 working days if this is shorter.
FOIA/ EIR - Internal reviews under	FOI	Government - central	FOIA There is no requirement under the FOIA to carry out an internal review, however the majority of public authorities offer some form of complaints procedure. The FOIA does not give a specific timescale for carrying out an internal review. If public authority offers the opportunity for internal review, the ICO considers that a reasonable time to complete a review is within 20 working days of the request for review, and that under no circumstances should the time taken exceed 40 working days. EIR Under the EIR, the public authority must offer an internal review (r11). If the requester wishes the public authority to carry out a review, they must request one within 40 days of receiving the public authority's response to their request. The public authority should respond to the request for internal review as soon as possible and within 40 working days. If the review upholds the original decision, the public authority should explain why this is the case to the requester. It is also good practice for the public authority to inform the requester of their right to complain to the ICO. If the review overturns the original decision, the public authority should release the withheld information, as well as acknowledging any other mistakes, and steps which will be taken to

			rectify these.
FOIA/EIR coverage - recent organisation changes	FOI	Government - central	FOIA - Now covers the following organisations:**ACPO (Association of Chief Police Officers), UCAS (The Universities and Colleges Admissions Service),FOS (Financial Ombudsman Service) Free schools** The First Tier Tribunal have allowed an appeal and held that the **Duchy of Cornwall** is a public authority under the Environmental Information Regulations (EIR). It is not covered by the FOIA.More details on the tribunalhere. **Royal Mail** and its subsidiaries ceased being a public authority following the sale of shares in October 2013. The Post Office remains a public authority.

Free Electoral Roll - FAQs	DPA	Internet & technology	**I have searched my name online and have found that Intelligent Tracing has a lot of information about me. Is this legal ?** In line with our regulatory activity we have been in discussion with these organisations. They are registered with us (the details can be viewed on the public register) and they have and continue to cooperate with us regarding the concerns raised. It would appear that they operate in a similar way to 192.com. That is, they gather information from publically available sources. In general this does not itself seem to breach the DPA. This is because in most cases getting info from publically available sources will be compliant with the first principle: The details appear to be gathered fairly, lawfully and a condition for processing can be satisfied (legitimate interest). However, we have been concerned in some circumstances about the apparent use of pre 2002 electoral roll information. People were allowed to opt out of the electoral roll that was available for commercial use, from 2002. In certain circumstances, the use by an organisation of an older version of the register may raise issues in relation to the processing of personal data, giving rise to a risk of a breach of the DPA. Such processing might be unfair as it may not be in line with the expectations of individuals. **I want my information removed from these websites. How can I do this?** We have received a number of enquiries about this issue. As you know there is no automatic right of deletion in the DPA. There was some suggestion that the owner of the companies was asking people to make a section 10 request if they wanted their information removed. Our view was that section 10 is only one way of considering whether the information should be removed, and we note that the 'bar' for a section 10 was often too high to be of practical use to people in these situations. Primarily, the organisation should consider whether it is 'fair' for the information to be included in the online directory in the first place – if not, it should not be processed online. Therefore, following discussions with the data controller, it has been agreed that they will remove details free of charge (via an online form) upon request. They also offer a telephone service for people to request removal, but please note this appears to be a premium rate telephone number.

			We have been advised by a few callers that the form for removal doesn't seem to work. There is nothing to suggest that this is being done on purpose, and may just be an IT issue. However if a person wanting to request removal, is unable to use the form, then we should provide them with the organisations address from our public register and advise the caller to write to that address with their removal request. **I have requested removal, but the data controller has asked me to supply lots of information that I am uncomfortable to give, and I believe it is excessive. Are they allowed to do this?** A data controller is allowed to ask for as much information as is reasonably needed to identify the person concerned. If you are being asked for more information than the website already has about you, this would appear to be excessive. We have explained to the data controller that he should only be asking for information that he already has in order to identify those making removal requests. **I have made a written removal request and they have not removed my data from the website.** Our view is that whilst there is no automatic right of deletion in the DPA. If a DC offers deletion/removal and then does not do it after receiving a written request, then this may constitute a first principle breach, and the individual can raise it as a concern with us in the usual way. **I want to know all the information that this company holds about me. How do I do this?** The individual can make a SAR in the usual way. Obviously the DC can charge the usual fee to comply with a SAR and may also request enough information to verify the identity of the requester and to action the request. **All of the above is as the matter stands at the moment. However, this is an ongoing matter and it is important to communicate that to any caller/enquirer.**

Gone away post and Telephone calls	DPA	Finance	Inaccurate Information - receiving mail at your address in someone else's name. There are circumstances when individuals will receive mailings to their address but the addressee has never or no longer lives there. In these cases we would consider this to be a compliance issue. The data in question doesn't identify the complainant albeit the information is incorrect (and would therefore be a P4 issue). In these circumstances we would ask the complainant to contact the organisation in writing to inform them of the inaccuracy. The DC should then mark their records appropriately to indicate that no further mailings should be sent to the address held. The DC can't delete or change the address details as they are receiving notice of the inaccuracy from a third party and not the individual directly. Inaccurate Information - receiving telephone calls for someone else - usually from debt collectors In this situation the householder would need to raise the issues in writing with the organisation concerned. The organisation should then mark their records appropriately to indicate that no further telephone calls should be made to that number. The organisation can't delete or change the telephone details as they are receiving notice of the inaccuracy from a third party and not the individual directly. If the Consumer Credit Act requires that certain communications are sent to a customer's last known address, then doing so will not breach the Data Protection Act.See full policy guidance below:- Consumer Credit Act requirements The Consumer Credit Act 2006 amended the Consumer Credit Act 1974 and introduced new requirements in respect of: Annual statements under fixed-sum credit agreements. (s6 CCA06 / s77A CCA74 requires these to be sent).Additional information in statements for running-account credit (which in accordance with s78 CCA74

			must be sent annually as a minimum, or whenever interest is charged or a payment is required from the debtor).Notices of sums in arrears under fixed-sum credit agreements. (s9 CCA06 / s86B CCA74 states they must be sent 6-monthly as a minimum).Notices of sums in arrears under running-account credit agreements. (s10 CCA06 / s86C CCA74 states these can be incorporated with statements).Notices of default sums. (s12 CCA06 / s86E CCA74 states these can also be incorporated with statements).Additional information in default notices.Notices relating to post-judgment interest. For all of the above notices, the CCA 2006 gives no timescale as to how long lenders can continue to send them. Breaches of the requirements usually result in the lender being unable to enforce the agreement for the period for which they are in breach. The Consumer Credit (Information Requirements and Duration of Licences and Charges) Regulations 2007 set out the content and forms of wording to be included in the statements and notices required by the CCA 2006, together with setting out the required form of the statements themselves. They came into force on 01 October 2008. Sending CCA-required correspondence to last known addresses Crucially, in relation to all the above, s176 of the CCA 1974 applies. This states that: "176 – (3) For the purposes of this Act, a document sent by post to, or left at, the address last known to the server as the address of a person shall be treated as sent by post to, or left at, his proper address". The following will hopefully elaborate and clarify further. The fourth principle of the DPA Whilst it is of course a relevant principle, we would not expect there to be a breach of principle four in most similar cases. To decide whether the address information is inaccurate or out of date, we would have to consider what the lender purports the information to be. Where the lender purports the address to be a 'last known address' (because they are aware that the address is not current) then this in itself is accurate and up to date. Even if the address details are deemed inaccurate, the fourth principle does allow for inaccurate or out of date data to be held, depending on the purpose for which it is used. In the case of debtors, in the absence of current address details, out of date address details are relevant for the original purpose of enforcing the credit agreement (as sending to a last known address allows lenders to fulfil their obligations

			under the CCA and therefore to continue to enforce the agreement). The seventh principle of the DPA This principle is also relevant in such cases as sending CCA-required correspondence to last known addresses does create a security risk of potential disclosure if the envelope is opened by the current occupant. Since October 2008 increased amounts of debtor personal data are required to be sent under the CCA, even to last known addresses, thus increasing the severity of that risk. It is true that the envelope should be sealed and that if the current occupant is not the addressee then they should not open it anyway, and could be committing an offence by doing so, but the reality is that people do open such letters (perhaps inadvertently, or to ascertain who the sender is in an attempt to stop the letters being sent). For the above reasons, we would suggest that both principles are relevant. Although the risk with regard to the seventh principle is only a potential one, it does have the potential for causing detriment to the data subject, especially if the current occupants of their previous address are known to them, or indeed the current occupant decided to use the details fraudulently. In summary, as long as lenders act appropriately in recording debtor addresses as out of date when informed as such, make reasonable efforts to trace the debtor's correct address and thereafter send only those notices and statements required by the CCA, containing the minimum information required by the CCA, we cannot maintain that a breach of the DPA has occurred.
Google Glass	DPA	CCTV & optical surveillance	Q. Are people going to be breaching the Data Protection Act when wearing Google Glass? A. If an individual is using Google Glass for their own use then they are unlikely to be breaching the Data Protection Act. This is because the Act includes an exemption for domestic purposes. However, certain uses of new technologies may cross over into regulated areas. Users of all video technology should be aware of their legal obligations when images are captured for non-recreational purposes. Q. What should a person do if they object to being filmed or photographed? A. Organisations using Google Glass to collect personal information must comply with the Data Protection Act. This includes making sure the information they are collecting is relevant, adequate and not excessive. If a person is unhappy with the way an organisation is handling their information then they should raise their concerns with the organisation in the first instance. If they are unhappy with the organisation's response they can raise the matter as a concern with us.

			If a person is unhappy with another person using Google Glass in a domestic setting, then a sensible first step might be to calmly raise their concerns with the Google Glass user, if it feels appropriate. While there may be an exemption for domestic purpose we would still encourage all Google Glass users should also respect individuals' privacy and understand that people's expectations around what is and isn't acceptable will differ depending on the particular situation or context. Q. Do you have any concerns over the privacy implications of Google Glass? A. As with any new technology that processes personal information Google must make sure that Google Glass operates in compliance with the Data Protection Act. This includes informing users about the way their information is stored and used by the company. While individuals using Google Glass for their own use will not normally be required to comply with the Act, organisations using Google Glass for business purposes will still need to handle personal information in the same way as they would for any other setting. For example, if an organisation's security staff are filming people using Google Glass then appropriate signage must be used to confirm that filming is taking place and the reasons for this. The information would also need to be kept secure and destroyed once it is no longer required. Q. What about the recent European Court of Justice ruling on the right to be forgotten? A. The recent ruling by the European Court of Justice required search engines to consider requests to remove search results that included information that is inadequate, irrelevant or outdated. This will include any Google search results presented to UK users wearing Google Glass. We are still considering the full implications of the judgment and our view is set out in our blog. Q. What about your ongoing enquiries into Google? A. Our investigation into data protection concerns relating to Google's privacy policy is ongoing.
Google Streetview	DPA	Internet & technology	We understand why people might have concerns about the Google Streetview service as it does involve capturing images of streets which may include someone's house, car or even an image of them walking on that street. In certain limited circumstances an image may allow the identification of a particular individual. However, we have spoken to Google and sought their reassurances that the product is not intended as a means by which individuals can be identified. In general terms it is clear that the service is aimed at capturing images of a location rather than of any individuals who happened to be at that location.

			Google have put in place safeguards to avoid risks to the privacy or safety of individuals. First of all faces and vehicle registration numbers are automatically and irrevocably blurred and individuals can report any image that is causing them concern and request that Google remove it. For example, if you saw an image that had not been blurred correctly, Google will blur it as soon as possible after you report it to them. Also the reporting mechanism allows you to report your concerns about any image not just ones relating to you. Some media reports suggested that the product could be used by people wishing to burgle houses on the basis that people are obviously out due to, for example, an empty driveway. It is important to note that images are not 'real time' and there is a long delay between the taking of an image and its publication so that it could not be used to make decisions about an individual's current whereabouts. In short we have seen the Google Streetview product and we are satisfied that it can operate within the provisions of the Data Protection Act 1998. At the point when Streetview is actually launched in the UK should you have any further concerns about a particular image you should first report it to Google. You would still have the right to complain to this office if you are not satisfied with their response.
Health and Social Care data breaches (IG Toolkit)	DPA	Health	All organisations processing health and social care personal data (excluding those in Scotland, Northern Ireland and Wales) must now use theIG Toolkit Incident Reporting Tool to report data breaches to the Health and Social Care Information Centre (HSCIC), Department of Health, ICO and other regulators. The Health and Social Care Information Centre (H&SCIC) has confirmed that smaller bodies such as opticians and dentists should also be using the IG toolkit as per the NHS procedure when reporting a security breach. If organisations are still in doubt, they should contact the H&SCIC helpdesk. H&SCIC has said that this does not negate any responsibility they may have to tell anyone else such as their Clinical Commissioning Group (CCG).

Health Services and Social Care Services - Definitions/differences	DPA	Health	The ICO holds the view that the definition in the DPA is not a complete definition or definitive list of medical purposes. Schedule 3, paragraph 8(1) DPA notes that the processing must be "necessary for medical purposes" and has to be undertaken by either a health professional or a person who owes an equivalent duty of confidentiality as that owed by a health professional. In light of the new legal duty for Local Government to integrate health and social care services it would perhaps be unrealistic and unhelpful for the ICO to adopt a very hard line upon the interpretation of Schedule 3 paragraph 8 to exclude any social care. Processing under Schedule 3, paragraph 8(1) such as the provision of care and treatment and the management of healthcare services covers services provided for the prevention, detection and treatment of medical conditions and associated healthcare (that is, for both physical and mental health and wellbeing) including social care which has a health focus or outcome, whether public or individual, and which is being provided in consultation with a healthcare provider. By way of further explanation, using the Shorter OED definitions, "medical" refers to "of or pertaining to conditions requiring medical…treatment or diagnosis." "social" refers to "of an activity etc.: performed to benefit or improve the condition of society." "social medicine" is defined as "those areas of medicine which aim to assist people with social or emotional problems, as psychology, psychiatry, etc." "social services" means "a service provided esp. by the State for the benefit of the community, esp. education, health, and housing." Social type medicine, using the OED definition above, which includes assisting people with social problems through the use of for example psychology or speech and music therapy would fall within the remit of Schedule 3, paragraph 8(1). Other social care services are provided for different purposes and in a different and arguably wider context. As noted above, unless there is an identified health element being provided as part of a social care service, we would not consider wider perhaps more traditional social care services to fall within the type of processing envisaged and permitted by Schedule 3, paragraph 8(1).

ICO and The Commissioner - FAQ	Other	Other	What is the Information Commissioner and ICO? The Information Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament. The Commissioner enforces and oversees the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003 within the UK and the Environmental Information Regulations 2004 and Freedom of Information Act 2000 within England, Wales and Northern Ireland. However, the ICO is also responsible for the EIR and FOI regulations in Scotland where the public authority is funded through an English PA E.g. The Forestry Commission, BBC Scotland and the Scottish Consumer Council, all of which are headquartered in Scotland but are subject to the FOI 2000 through their relationship with their parent body.) Who is the Information Commissioner? Christopher Graham is the current Information Commissioner. He is an independent official appointed by the Queen. What does the Information Commissioner's Office do? The Information Commissioners Office is a UK independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the legislation which we oversee is not complied with. Our main functions are educating and influencing (we promote good practice and give information and advice), resolving problems (we resolve eligible complaints from people who think their rights have been breached) and enforcing (we use legal sanctions against those who ignore or refuse to accept their obligations). Relationship with the Ministry of Justice

			The ICO is an independent public body and the Ministry of Justice is the ICO's sponsoring department within Government. Lord McNally is the Minister with responsibility for Data Protection and Freedom of Information within the Ministry of Justice. Chris Grayling is Lord Chancellor and Secretary of State for Justice. Regional Offices The ICO is based in Wilmslow, Cheshire but also has regional offices in Northern Ireland, Scotland and Wales. These were established in 2003 as a direct response to the devolution process and enable us to provide relevant services where the legislation or administrative structure differs. The appointment of commissioner is made by the Crown. But who proposes the commissioner? Does he have to fulfil some conditions (education, no crime record?) No one nominates the Commissioner. It is an open recruitment process. Any candidates who would like to be the Commissioner simply apply and go through the recruitment process. The process is run by the ICO's sponsoring government department, the Ministry of Justice. The successful candidate from this process has to appear before a committee of Parliament (pre-appointment scrutiny), who produce a report on their suitability for the post and any recommendations. This report is not binding. Following this process the government then decides whether to put them forward as the person for the Crown to formally appoint. Removal (dismissal) of the commissioner. The Commissioner can only be removed from office through the addresses of both houses of Parliament and by the Queen. The reasons for such a dismissal would have to be gross misconduct. Parliament approves the budget. But who proposes the budget of commissioner? The Budget is negotiated between the ICO and the Ministry of Justice. This proposal is then submitted to Parliament for agreement. Appeals against the ICO go to tribunal. How long does the tribunal have to decide on appeal? Are there any fees? If the appeal continues to Court of appeals, are there timelines and fees? The time it takes for an information tribunal to hear and decide a case will depend on the complexity of the case. The Information Tribunal is free of charge to the complainant. It is very rare for costs to be awarded against the losing party in the Tribunal, this is because the party has to

			have acted unreasonably for them to be awarded against them. It is the same position in the next tier, the Upper Tribunal. In the next tiers of appeal – the Court of Appeal and Supreme Court, the traditional position of the "loser pays" is followed, unless a protective court order is agreed in advance e.g. both parties agree to cover their own costs and not seek costs against each other. What sanctions could apply for none compliance with a decision, information or enforcement notice? If an organisation does not comply with an Freedom of Information Act enforcement notice or decision notice served by the ICO then this is seen as a 'contempt of court'. This matter is then referred back to the Tribunal or the Court for action which could then result in a fine for the public authority. To date the ICO has not had to formally instigate these proceedings because compliance levels are high. Is somebody, (ICO, or ministry) responsible (obligated) for educating public authority officials, or for raising awareness in public? Under section 47 of the Freedom of Information Act it ispart of the Information Commissioner's responsibility to raise awareness for both the public and public authorities.
ICO register of data controllers. Viewing and use of.	Other	Other	How can I search/view the ICO register of data controllers? Under section 19 of the DPA we are required by law to make the register available for inspection and currently do so via our website. A copy of the register is also available on DVD if anyone would like to request it. The register is made available in two forms, a short form and a long form, each extracted in XML format on a monthly basis. Can I use the information found in the Information Commissioner's Register of data controllers on my website? The register will be provided under the Open Government License and may be reused provided that the reuse of any personal data complies with the requirements of the Data Protection Act and, in particular, that such data are not used in a way that is inconsistent with the purpose for which the register was created. For example, not used for direct marketing, or in a way that otherwise adversely affects the privacy of individuals. Before reusing any of the information contained in the register, they should familiarise themselves with the license conditions. The license terms are available at the following URL:

			http://www.nationalarchives.gov.uk/doc/open-government-licence/ It is also worth noting that the ICO register of data controllers is updated regularly. It is therefore likely that if anyone puts any of the register on their website, that it will quickly become out of date.
Location Data and Smartphones	DPA	Internet & technology	Information relating to the location of a smart phone is likely to be considered personal data.This is because Smart mobile devices are inextricably linked to an individual. The movement patterns of a smart phone can provide an intimate insight into the private life of the owner.Smartphone manufacturers, or app developers, must obtain consent before collecting location data. They also need to be clear and transparent about the purpose of collecting the data.Organisations are not able to rely on consent obtained through general terms and conditions.By default, location services should be switched off. Individuals should also be able to turn off location services at any time.More information can be found in the Article 29 Working Party's guidance on geolocationhttp://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

London Gazette bankruptcy records	DPA	Finance	It is our understanding that essentially the concern being raised is that the archive of back copies of the London Gazette is available online. This means that details of bankruptcies reported in the Gazette will in theory be available to anyone searching for information about the individuals concerned even after the date the bankruptcy has been discharged. Whilst we can certainly appreciate the reason that individuals would be unhappy with their information being available in this way, we do not believe that ultimately we would have any basis to require that the London Gazette (or any other publication) does not make available any back copies of their publications online (or that they remove all personal data from old copies of newspapers or magazines). It is common practice now for newspapers and other publications to put their archives online, this is information that has been published and is widely available and it is now a historical record that can be accessed on the internet. The way the internet works means that records like archived copies of newspapers or magazines which would always have been available for people to use and access if they wanted to (for example in libraries) are now in practice more easily searchable which unfortunately will mean that information like this may be more easily accessible. NB - Some roles (Army Officer, MP) require that the individual has never been made bankrupt. Therefore some public record of all historical bankruptcies may be of use.

MPs and Constituent's Complaint Files	DPA	Political parties	Internal guidance only Whilst this information is freely available to Members, it is not published on our internet and it is asked that you do not share it verbatim with a requester. As you know Members are data controllers in their own right and are not obliged to follow House policy or guidance, particularly for information relating to constituents. Parliament's guidance, which is available to Members, runs along the following lines: Handling personal data if a Member dies or leaves mid-termConstituency casework may be handled until the end of the fourth day after a new Member is elected for all constituents who are content for this to happen. If there is any doubt, consent should be sought.The records held should be reviewed in line with the guidance below. Reviewing recordsA former Member will continue to be the data controller for all paper and electronic records that they hold and they must therefore be sure that anything they do with their records is in line with the expectations of the individuals concerned. For example, constituency casework records should not normally be passed on to a new Member or to a history centre/county archive unless the constituent is happy for this to happen.Records relating to closed cases which are not likely to be reopened should usually be securely destroyed.Live cases, and closed cases which are likely to be reopened, should be assessed on a case-by-case basis, considering the expectations of the individuals and consulting with them where their views are not clear.Options that could be offered to constituents include: - Destroying the case-file - Passing the case-file to the new Member - Passing the case-file to the constituent themselves - Template forms for a constituent to indicate their preference can be found in the guidanceIf a case-file is to be passed on, either to the new Member or to the constituent, it should be checked first to ensure that it does not contain any confidential information which either party should not see. (Further guidance available to Members) Explicit consent from the constituent is always needed to pass on cases containing sensitive personal data to a new Member. Notification to the Information Commissioner should be reviewed.

MPs and Elected Representatives - Disclosures to	DPA	Political parties	**Disclosures to Elected Representatives - Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002. S.I.2002 No. 2905** Background This Order was introduced because Members were concerned that the requirements of the Data Protection Act 1998 were providing an undue hindrance to their work on behalf of constituents. It was intended to remove unnecessary bureaucracy and delay. However, in Standing Committee attention was drawn to the need to ensure that the response to the problem was proportionate, and that individual constituents and others do not feel that their privacy is being affected unreasonably by the Order. It would, therefore, be most helpful if Members inform the Lord Chancellor or the Commissioner of any instances where a constituent is unhappy about disclosures of sensitive personal information made in the course of constituency casework, whether by Members or organisations responding to them. Line to take We need to cover the following points when advising about disclosures of personal data to elected representatives (Members of Parliament, elected Council representatives etc)) A data controller is not compelled to disclose information to an elected representative by this order If a data contorller wishes to disclose personal information to an elected representative it may not be necessary to seek the consent of the data subject if they are satisfied that the disclosure is necessary to enable an elected representative to deal with casework on behalf of their constituent (the data subject) The order enables a data controller to satisfy a condition for processing sensitive personal information without the need to seek the consent of the data subject (the constituent).This doesn't automatically mean the processing is 'fair' and 'lawful' as requried under the first principle but in most cases it will be considered 'fair' to disclose without informing the data subject. However, care should be taken in those cases where the data controller feels they may be about to disclose more information than the data subject might reasonably expect. For example: Constituent seeks assistance from MPMP approaches Data Controller and asks for information about issueData Controller holds information that they believe the constituent might not have anticipated would form part of the information to be disclosed as part of the MP's request.If a data controller is in any doubt either as to the legitimacy of the request or the information they feel they would be disclosing in order to comply with it they can of course seek the data subject's consent.

National Insurance Number as an identifier - DWP	DPA	Government - central	Background The ICO has previously considered whether the DWP are in breach of any DP principles when they use the National Insurance Number as an identifier when paying benefits / pensions. We have also received complaints previously about the NiNo being quoted on bank statements when these payments are made. Line to take The use of the National Insurance Number by various parts of the DWP when making payments (benefit or pension) to individuals. We understand that the DWP, who administer (own) the National Insurance Number, use it as their prime identifier for individuals – as opposed to names. They consider it to be a main identifier whereas a person's name is not –at least not sufficient for their purposes. We understand that it is the DWP who determine how and when the NINO is used in order that it is properly managed and controlled to ensure that:the right record is identified quickly and effectivelythe right transactions are carried out to the right recordsthe right decisions are made about entitlement to National Insurance based benefitsthe right decisions are made on applications for other benefits, tax credits and child maintenanceNational Insurance and taxes are collected from the right people at the right time. We do not consider that the use of the NINO by the DWP is likely to fail to comply with the provisions of the Data Protection Act 1998. When making payments directly into a bank account the DWP are effectively using an appropriate identifier for their payment records with a traceable audit trail should it be required. Of course, if the information were to be transmitted by the DWP to the wrong bank, or to an unauthorised third party, then there would be further issues for the ICO to address. The bank must keep the personal data that they receive secure. Disclosing the NINO to individuals in their bank statements would not appear to us to raise any data protection issue over and above disclosing other information in the statement – for example payments, account numbers, sort codes and transaction details. We understand from colleagues who deal specifically with the banking sector that it is not an unusual practice and is not considered to be likely to contravene the data protection principles.

Occupational health referrals and data sharing	DPA	Employment	The Access to Medical Reports Act 1988 applies when an employer seeks a report from a worker's GP or any other medical practitioner who is or who has been responsible for the clinical care of the worker. In summary, the obligations on the employer are to:-Notify the worker of his intention and obtain the worker's consent to the application for a report;Inform the worker of his or her right to:Withhold consent to the application being made;Access the report before it is supplied to the employer by telling either the employer or the medical practitioner of his/her wish to do so;Withhold consent to supply of the report to the employer once he/she has seen it;Request amendments to the report before it is supplied;Access the report for up to 6 months after it has been supplied by the medical practitioner. Workers should not normally be asked to consent to the disclosure of their entire general practitioner records or other comprehensive care and treatment records such as those held by a hospital. Although on occasions an occupational health physician may need access to the full record, such records contain more information than the employer is ever likely to need. Where it is necessary to seek information, the GP should be asked specific relevant questions to elicit the information needed by the employer. Occasionally, an employee may decide to withdraw consent for their employer to process the personal data contained within an occupational health report after the report has been disclosed to the employer. Depending upon the circumstances, the employer may still be able to rely upon other scheduled conditions to continue to process the personal data (even if consent has been withdrawn). The individual employee would still retain their right to make a Section 10 request to their employer.
Opt-Out UK Ltd	DPA	Direct marketing	Background The issue about Opt-Out UK Ltd is that these requests state that processing should stop for the purposes of direct marketing and not just for certain types / formats as was the case with the Green Preference Service (and therefore not legitimate section 11 requests). We assume that this organisation is sending names in bulk to data controllers (as GPS did) therefore situations may arise where section 11 requests are going to companies who are not processing the relevant data subject's personal data. This raises the question of whether data subjects are aware that their personal data will be potentially sent to companies who have no record of them. This issue has been flagged to the relevant SL team. They can decide whether direct contact with the organisation is necessary. **(Background information for internal use only)** Line to take In principle, as long as the requests are an accurate reflection of the data subjects wishes in relation to direct marketing and fulfils the other aspects of section 11 eg is in writing, then such requests can be made on the data subject's behalf in this way. However, data controllers who have genuine concerns regarding whether an

			organisation is truly representing a data subject is well within their rights to refuse to comply with one of these requests until it is satisfied. It may even be reasonable for an organisation to contact the person directly to check the status of the request. It is important to note that the section 11 right does include a request to not begin marketing, so it must follow that even if there is no record of the person in a database, their details should still be added to a suppression list if possible.
Planning Applications / Disclosures	DPA	Government - local	Background When a planning application for building work etc is submitted to a council planning department, this information is usually made available to the public via council websites, public libraries and notices in the local press. Also: If a person registers an objection with the local planning authorities, regarding a planning application then the details of the objection (including some details of the person making the objection) will be passed to the applicant. Line to take Application There is a requirement under the Town & Country Planning Act 1990 to make certain details relating to planning applications (including some details of the individual making the application) available to the local community.As the council has a legal obligation to make certain information available to the public it is unlikely that this would constitute a breach of the Act. As section 34 of the Data Protection Act (the Act) will apply.As section 34 includes an exemption from the 'subject information provisions' where information is required to be made available to the public by enactment, the council **would not** be obliged under the DPA to provide fair processing information to an individual submitting a planning application. However the ICO would always encourage the council to provide such information. Disclosure of Objections to Application Again, as the disclosure to the applicant would be a requirement of the Town & Country Planning Act 1990, section 34 of the Act will apply.Therefore as long as only the information as required by the Town & Country

			Planning Act 1990 is provided to the applicant it is unlikely to constitute a breach of the Act, regardless of whether fair processing information has been given to the complainant. However, again, the ICO would always encourage the council to provide such information.Therefore we would always advise that the council provide fair processing information when an individual submits a response to a planning application, although this would not necessarily be required by the Data Protection Act. Publication of planning applications on the internet Local Authorities now commonly publish details of planning applications on their websites. Specific regulations allow them to do this. However, not all of the details provided by applicants have to be published. By simply scanning whole applications and putting them online, Local Authorities risk publishing (and making widely available) excessive information such as signatures, email addresses, home telephone numbers and even medical details. This is not only an unwarranted intrusion into applicant's privacy but could in extreme cases expose individuals to the threat of identity fraud. Local Authorities must ensure that individuals have prior notification (i.e. provide fair processing information) that their planning application will be published on the internet as it is unlikely to be obvious to individuals that this will happen. While the planning process has always been an open one, Local Authorities have only relatively recently harnessed technology in this way to increase public participation and maximise transparency. Councils should also have a quick process in place to remove any excessive information quickly. Publication without redaction If a council is planning to change their procedures to publish planning information without redaction they should only do so after assessing the risks and taking steps to minimise them. They should: carry out a privacy impact assessment;give a fair processing notice saying the information provided will be published online without redaction; andtake steps to minimise the personal data they collect. These steps alone will not ensure compliance with principles 1 and 3.

Police & Crime Commissioners FAQs (PCC)	DPA	Police, legal & criminal justice	Q) What is a Police & Crime Commissioner (PCC)? A)Police & Crime Commissioners are individuals elected to office by the public with the aim of ensuring that police forces are tackling issues important to that community. In London it is known as 'the Mayor's Office for Policing & Crime'. The position was created under the Police Reform & Social Responsibility Act 2011. Q) What will they do? A)PCCs will have a broad range of powers around ensuring that local policing needs are met. Broadly these will cover:Holding the chief constable to account for the delivery of the force (including appointing and, where necessary, dismissing the chief constable).Setting and updating a Police & Crime Plan.Setting the force budget and precept.Regularly engaging with the public and communities. Q) Are they covered by the Data Protection Act and the Freedom of Information Act? A) PCCs will inevitably keep records about their staff, their professional contacts, members of the public and others. Therefore they will be processing personal data and will be 'data controllers' for the purposes of the Data Protection Act. We have advised the Home Office that PCCs will be data controllers in their own right and will be required to notify with our office and to comply with the data protection principles. Schedule 16, part 3, Section 249 of the Police Reform & Social Responsibility Act 2011 amends schedule 1 of the FOIA to include PCCs and The Mayor's Office for Policing & Crime as public authorities for the purpose of the FOIA. Q) Aren't PCCs already required to publish certain information? How does that affect their FOI responsibilities? A) PCCs will have a statutory duty to publish certain information covering a wide range of areas. These include number and make up of staffNames, salaries and contact details of certain staff membersInformation around income and expenditureDetails of contracts entered into above a certain value (£10,000)Details of certain meetings held and decisions made. We have made it clear that this does not absolve them of their responsibilities under the FOIA in respect of publication schemes but sits alongside it. In addition, they may well receive FOI requests for information which falls outside the information they are required to publish.

			Q) Don't Police Authorities already do a lot of this? A) Police authorities are being abolished and some, though not all, of their functions are effectively transferring over to the PCCs. In particular, most of the Police Authorities' legacy files will be transferred to the PCCs meaning they will become the data controller for this information, which may also be the subject of FOI requests. Q) So, if PCCs are holding the Chief Constable to account and setting the forces budget and priorities, are the Police Force just a data processor? A) The relationship between the PCC and the Chief Constable, particularly in terms of who will be responsible for what and so who will be the data controller, is complex and we are still discussing this with the Home Office. However, broadly speaking at this stage we envisage that the Chief Constable will remain as data controller for at least some of the information which the force holds. Exactly what that information will be may vary from force to force depending on the PCC, their priorities and what, if anything, they have expressed interest or desire to have control over. However, given the nature of their roles, we do not consider any of the parties involved to be data processors. Q) Who will hold the PCC to account? A) The Police Reform & Social Responsibility Act 2011 also makes provision for the creation Police & Crime Panels (PCPs). Their role will be to scrutinise the conduct and performance of the PCC. Q) What happens if a Police Authority was dealing with an FOI request or a SAR at the point that it was abolished? A) Where a public authority is discharging the functions of a dissolved public authority, the responsibility for dealing with a request received by the dissolved public authority passes to it. In many respects, a PCC will be discharging functions previously discharged by Police Authorities and so a request which was being handled by a Police Authority at the point at which it is abolished would pass to the PCC.

Police retention of data.	DPA	Police, legal & criminal justice	The issue of how long personal data can be retained for actually varies depending on the type of personal data in question. In the main, the way in which the police handle information (including personal data) is set out in the Management of Police Information (MoPI) Code of Practice. The Code sets out a minimum retention period for police information of 6 years. Once 6 years has elapsed, there are requirements to review the information but if it is deemed to still serve a policing purpose (which are also defined in MoPI) then it can be retained. MoPI does not apply to the retention of information on the Police National Computer. Records on the PNC are retained until the subject is deemed to have reached 100 years of age. This policy was affirmed by the Court of Appeal in Chief Constable of Humberside & Others v Information Commissioner. Who is the data controller for the Police National Database and the Police National Computer? The data controller for the Police National Database (PND) and the Police National Computer (PNC) is thatall forces are data controllers in common. SAR should be made to ACPO.
Police retention periods - DNA, PoF Act and Biometrics	DPA	Police, legal & criminal justice	The Protection of Freedoms Act implements the commitment by the coalition government to reform DNA and fingerprint retention so that only people who are convicted of an offence will have their material retained indefinitely. This is in response to the judgement in the S and Marper v UK case (30562/04 [2008] ECHR 1581 (4 December 2008)), decided by the European Court of Human Rights, which held that holding DNA samples of individuals who are arrested but later acquitted or have the charges against them dropped, is a violation of the right to privacy under the European Convention on Human Rights. The model laid out in PoFA is not straightforward and is based on age of offender, seriousness of offence and whether or not the individual is charged or convicted. Further, the DNA and fingerprint deletion provisions will not be commenced until October 2013. Current position Although the provisions haven’t been commenced as yet, there has been a program of deletions going ahead

			prior to commencement. All unreconciled DNA profiles have now been deleted from the National DNA database (these are those profiles that aren't connected to a PNC record). The deletion of unreconciled fingerprint records will start shortly. The next stage of deletions will be of those individuals who have had a single arrest resulting in no further action (NFAs). This started on 3rd April 2014. Fingerprint deletion for single arrest, NFAs started on 1st May 2014. Samples PoFA only allows samples to be retained for six months. This allows enough time for the profile to be derived from the sample and uploaded to the DNA database. All legacy samples are currently being deleted and over 1 million samples have been deleted so far. Samples may also be held locally. These must also be deleted when the provisions commence and Chief Constables will be held to account for any illegally retained samples. Retention periods for DNA profiles and fingerprints from October 2013 ConvictionsAdults – will be retained indefinitelyUnder 18s – serious – will be retained indefinitely if a 'qualifying offence' (serious violent or sexual offences, terrorism, burglary offences)Under 18s – minor – if first conviction (retained for five years plus length of custodial sentence), indefinite if custodial sentence of five years or moreUnder 18s – second conviction – indefinite Non convictions'Qualifying offence' – arrested and charged – three years plus possible two year extension by Court'Qualifying offence – arrested but not charged – can be held until 'end of investigation' or possible three years on application to the Biometrics Commissioner (indefinite though if already convicted for a recordable offence), plus two year extension possibleMinor offence – Penalty Notice Disorder (PND) – two yearsMinor offence – arrested or charged – none but speculative Information also available via Merideo link: Protection of Freedoms Act and Biometrics retention periods

Publication scheme for EIR	EIR	Government - central	The EIR require public authorities to make environmental information readily accessible in an electronic form, and to take reasonable steps to organise information to allow it to be published systematically and proactively (r4). All environmental information should be published unless:it was collected manually pre 2005,it would be withheld under an exception,it is archived and difficult to access, orit is personal data. There is no requirement to follow a publication scheme, or guide to information, but it is good practice to do so and may help the public authority to comply with the requirements of the EIR. The definition documents produced in relation the FOIA also cover environmental information.
Recording calls and Fair processing	DPA	Internet & technology	Whilst recording a telephone conversation without the knowledge or consent of an individual may affect someone's privacy, it does not necessarily breach the 1st principle of the Act. The Act does not require that an individual is told specifically that their conversation is being recorded. The requirement relates more to the purposes of the recording. There is a requirement to inform individuals if the recording is to be used for a purpose different from the purpose of the original telephone call in so far as this would be outside the individual's reasonable expectations. There is often some confusion around what sort of purpose would we consider to be outside of people's reasonable expectation (ie when would you have to inform people) in particular whether using recordings for staff training is a different purpose. The ICO's view is that it is not generally unreasonable to expect a call from a call center to be recorded for training purposes. Although the individual has not necessarily been told what the recording is going to be used for, the activity of recording calls for training purposes is not inherently an unfair use of the recording. While it does appear that the purpose of the recording is different from the purpose of the original telephone call, we would not consider it beyond reasonable expectation for the individual to expect this call to be used for training purposes, (especially if the data controller had taken steps to notify callers elsewhere such as in mailings or on their website.)
Refusal notice format / contents under FOIA/EIR	FOI	Government - central	FOIA Where applicable, a written refusal notice must be issued within 20 working days (s17). It must include:The exemption being applied (including subsection)Details of why the exemption is being appliedConfirmation or denial of whether the public authority hold the information requested (except where exempt)Details of how

			to request an internal review (if applicable)The requesters right to complain to the ICO If a public interest test is required, the details of this should be included in the first refusal notice, or, if the authority extended the time for compliance to determine the public interest, the second refusal notice. If providing information about the public interest test would require disclosure of exempt information, then the public authority doesn't have to provide it. EIR Where applicable, a written refusal notice must be issued within 20 working days (r14). It must include:The exceptions being applied (including subsection)Details of why the exception is being applied (except where the request relates to national security)Details of the public interest test (except where exempt)Confirmation or denial of whether the public authority hold the information requested (except where exempt)Details of how to request an internal reviewThe requesters right to complain to the ICO
Reproduction of information from Twitter	DPA	Internet & technology	The below applies where we receive enquiries/calls about reproducing 'Tweets' (or prospectively any other information put publicly on social networks). Line to take Essentially this situation is not very different from other situations where data controllers want to use information which is in the public domain. The DPA still applies to their further processing of the information so you need to consider the fairness issues. (This assumes that broadcasting a tweet = processing personal data, which it may not necessarily be due to the fact it might not identify a living individual). Whilst you do not necessarily need to obtain consent in every instance of reproduction of specific Tweets, you should definitely consider individuals reasonable expectations. The nature of Twitter – it's nature as a conduit for one to broadcast ones opinions to the world means that it might not be unreasonable to use a tweet more widely, but it depends on the circumstances. For example, if two people are having a conversation over Twitter it might not be fair to broadcast it without telling them, but if someone has used Twitter to comment on something in the news then broadcasting might not be a problem. Then you need to decide whether it would be fair to broadcast it. This could well depend on the context of the show. Two examples: If the shows intentions are to humiliate an individual that probably won't be fair; alternatively if it's to cover opinions on a current news event then it is more likely to be reasonable.

Requests for a list of public authorities under EIR	EIR	Government - central	Under Directive 20034EC Article 3.5.b EIR it states: For the purposes of this Article, Member States shall ensure that: .... (b) lists of public authorities are publicly accessible; Some times we are contacted asking for such a list. The answer is essentially: Yes, that is what the directive says. But the ICO don't hold the list. Whilst the ICO regulates compliance with the FOIA in this country, the ICO is not responsible for implementing the directive into law. DEfRA are the Government Department responsible for the EIR in that way.
Retention P.5 DPA	DPA	Other	It would be impractical for the Act to be able to give specific retention periods for every type of organisation that must comply with the Act. Therefore the fifth principle means in practice that once it is no longer necessary for a data controller to retain data collected for a particular purpose, they should take the appropriate steps to dispose of it. In order to comply with the principle, the Data Controller should have a system for the removal of different categories of data from their system after certain periods. Things to consider are:Legal liability (for employees, or advice given, or work done).Requirements of a governing body.Other legislation.Expectation / any fair processing given. For instance, a Data Controller may have personal data regarding employees that have left the company. If they are no longer employing the individuals then it is not necessary for them to still retain some data after the time limit for an employment tribunal has passed, (eg PDRs, 1-2-1s, training plans). However some information may need to be kept (for references, pension provision). The controller should be aware that there will be other legislation (employment law, tax law etc) that requires them to hold data for a statutory period, and they should also take this into account when deciding on their own retention periods. When responding to questions in relation to retention, the following guidance may be helpful;http://www.nationalarchives.gov.uk/documents/information-management/sched_internal_audit.pdf

Retention and Copying of original documents	DPA	Employment	The Data Protection Act itself would never require the retention or copying of original documents. The DPA does not specifically talk about the copying or retention of original documents. The Act applies to the processing of personal data, and a data controller would need to ensure that they complied with all the principles of the Act, and in particular the 'fair processing', and the 'conditions for processing', aspects of the first principle when processing passport or birth certificate information. The third principle would also apply when seeking to determine whether the information in question was relevant given the purpose for which it was intended to be used. The fifth principle also applies when seeking to determine how long the information should be retained for. In some circumstances (particularly employment) a data controller may be under a legal obligation to check (and subsequently prove that they have 'checked') the legal status or identity of a data subject. In these situations it will obviously be easier for them to rely on a condition for processing, but they would still need to supply fair processing information and comply with all the other principles of the Act (retention, security etc). Important Point: When asked about the retention or copying of original documents the first thing to ascertain is why the data controller requires this information. Once that is clear, it is easier to ascertain whether it is likely that the data controller will be in compliance with the Act.
SAR and third party data - summary	DPA	Other	The first consideration for a data controller is: Can the request be responded to without disclosing the information about the third party? This doesn't just mean the name of a third party. A third party may be identified from other information unique to them, such as a job title and in other situations where the person making the request could access other information relatively easily to help them identify the third party. If the request cannot be responded to without disclosing any third party information s.7 (4) of the Act means that the data controller must consider: Whether consent has been given by the third party to disclose? If not, is it reasonable in all the circumstances to disclose the third party information without consent? Please note - consent does not have to be sought before considering this. Point 1 is simply to check if consent has already been provided. Section 7 (6) of t he act provides some factors which a data controller should consider when seeking to determine whether it would be 'reasonable in all the circumstances' to disclose third party information. The

			list is not exhaustive: any duty of confidentially owed to the third party any steps taken by the data controller to seek the consent of the third party whether the individual is capable of giving consent any express refusal of consent by the other individual In summary - unless there is a compelling reason not to disclose the third party information the ICO would generally encourage disclosure.
SAR by a Trustee of a debtor in bankruptcy	DPA	Finance	A trustee of a debtor in bankruptcy can request information from a mortgage advice company under Section 366 of the Insolvency Act 1986. However, some mortgage advice companies have claimed that Section 7 of the Data Protection Act 1998 (DPA) overrides the Insolvency Act 1986 and have requested a fee of £10 to provide this information. ICO Response: The DPA is not intended to interfere with any other laws or pieces of legislation and will not stop or prohibit an organisation from releasing information if another law compels them to do so. If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access. However, the exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about an individual, the additional data is not exempt from the right of subject access even if the organisation publishes it. However, the ICO cannot advise on the obligations which Section 366 of the Insolvency Act 1986 places on an organisation. If it places a legal obligation on an organisation to release information free of charge, then the DPA will not interfere or prohibit this. Trustees should be advised to contact the body responsible for regulating the Insolvency Act 1986 to clarify the obligations on an organisation under Section 366 and, if necessary, raise a complaint with that regulator if the request is refused.

SAR Counting the 40 days to respond. (General + Schools)	DPA	Education	The duty on the data controller is to comply with the applicant's request within the 40 day prescribed period. We take that as meaning that the data controller has to send the personal data to the applicant within the 40 day period, rather than meaning that the applicant must receive the personal data within that period. Although DPA 7(1),(c) says the data subject's right is to have the personal data communicated to him within the prescribed period, we would not interpret this as meaning that the communication has to be completed within that period. The practicalities need thinking through here – if the communication had to be completed within the 40 day period would this mean that overseas subject access applicants have to have their application expedited because it takes 2 weeks for the mail to be delivered. Or would we expect applications to be handled more quickly at Christmas because of postal delays? No, we wouldn't. Schools. Regardless of whether a school is closed for the summer holidays if they receive a valid SAR then they will have the normal 40 days to comply. There is no provision within the DPA for the 40 days to start when the school reopens. Obviously if it is a request for educational records held within a state school then the 15 school days will apply. **NB** Whilst we can sympathise with schools about this issue if we do receive a complaint about a subject access being complied with outside 40 days which has been caused by the school being closed then we will have to make a compliance unlikely assessment.
SAR fee - acceptable payment types	DPA	Other	Background If a data subject provides the correct fee in a format which is legally recognised in the UK to denote payment eg cash, cheque or postal order etc. and assuming that they have correctly provided all the other elements of a subject access request eg adequate identification etc, the moment the data controller has received the request (section 7(2)), its obligations under section 7 begin. Line to take A data controller does not have to accept the payment, but the obligation begins nonetheless – acceptance is

			not a condition of receiving. A data controller is well within its rights to state a preference for a particular format of payment, but it cannot demand it.
SAR Handling repeated requests	DPA	Other	Preparation Responses to all SARs should be comprehensively documented. In the event of a repeat SAR the only information which the data controller is obliged to consider is information that has been amended, received or created since the last SAR was dealt with. Careful documentation of responses will ensure that any new information can be provided quickly. It is also good practice to record when any exemptions which have been relied upon to redact information from the response together with a brief note showing why the data controller believes these exemptions apply. Is it a new SAR? Where a data controller believes it has already given an individual all of the information they are entitled to see it will not be unreasonable to ask the requester why they have made a repeat SAR. It may be that the requester believes some information has been incorrectly redacted from the original response. At this point any notes made for the original SAR will be useful. Alternatively a requester may believe that documents which should have been included in the response are missing. In this case the data controller is entitled to ask for a description of the documents, the date the requester believes they were created, information about where the requester thinks they might be stored and any other information which might assist in locating the document. S7(3) of the Act is clear that where a data controller "reasonably requires" further information in order to locate the information the requester is seeking then, where the requestor has been informed of this, the data controller is not obliged to deal with the SAR until that information has been received. Reasonable interval It may be that an individual submits a repeat request very soon after their original request. Under s8 (3) and (4) of the Act a data controller is not obliged to comply with a repeat SAR unless a "reasonable interval" has elapsed since compliance with the previous request. Data controllers might want to consider how this is covered in their policies and procedures.

			In determining a reasonable interval a data controller must consider “the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.” With this in mind a data controller may wish to consider applying different intervals to particular files rather than simply setting one blanket interval to cover all files and all repeat SARs. Fees Data controllers should also bear in mind that all repeat SARs will be subject to the fee as outlined in S7(2)(b) and they are not obliged to deal with any request unless they have received the fee. The fee may be claimed even if there is no information to be forwarded in response to an SAR. Managing In cases where a single individual is sending numerous or frequent repeat SARs to different departments or members of staff the data controller may wish to appoint someone to be a single point of contact for the requester in order to co-ordinate any necessary searches of the data controller’s files, the collection of any necessary further information and fees from the requester and the responses to the repeat SARs. Protracted correspondence In some cases individuals may continue to send repeat SARs even when all the relevant files have been disclosed. Complaint files are a good example. These may be updated and added to at regular intervals while the complaint is ongoing, but at some point the data controller will feel that the complaint has been dealt with and will close the file. Once this happens, if repeat SARs continue to be made, then the only information being added to the file may be correspondence from the requester. In these cases, where the data controller has reason to believe that the requester has copies of this correspondence, it may comply with the SAR by sending the requester a letter explaining that there is no new information on file that the requester does not already have. It is not necessary, in these circumstances, to send copies of the requester’s latest correspondence. The Act does not insist on the provision of documents to a requester, only on the disclosure of information which the requester is entitled to see but does not have in his possession. End of the process In some cases individuals may make repeat SARs because it is their view that information is being withheld from them in breach of the Act. If this is the case data controllers can refer them to the ICO once they have exhausted your own complaints procedure.

SAR Health Records Fees	DPA	Health	Subject Access Fees for MRI Scans/X-rays If the data is held in electronic form, the maximum fee that can be charged is £10. If the data is printed out or only held in manual form, then a maximum fee of £50 can be charged. Maximum fee A maximum fee of £10 may be charged for granting subject access to health records that are being **automatically processed** (or that are recorded with the intention that they be so processed). A maximum fee of £50 may be charged for granting subject access to manual records, or to a mixture of manual and automated records, where the request for subject access will be granted by supplying a copy of the information in permanent form. A fee can be charged to view your health records. The charge for electronic, manual or mixed format records is up to a maximum £10 charge, **unless** the records have been added to in the last 40 days in which case there should be no charge.
SAR Information exempt as may cause harm - Education.	DPA	Education	Paragraph 5(1) of the Data Protection (Subject Access Modification) (Education) Order 2000 states that: "Personal data to which this Order applies are exempt from section 7 in any case to the extent to which the application of that section would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person." The provision makes reference to "…in any case to the extent to which…" which clearly indicates that the provision is meant to only apply to the release of personal data in an education record where it is likely that serious harm will occur. If there are parts of a document where this is clearly not the case, then the exemption does not apply. It cannot be used as a blanket reason to withhold an entire document unless that entire document fulfils the test within the provision. In principle, the ICO reserves the right to challenge the opinion of anyone in relation to the discharge of our duties where we have reasonable grounds for doing so. However, in practice, when it comes to the view of a medically qualified professional eg a doctor, in relation to matters involving the physical / mental condition of an individual - we are likely to take their word in light of their specific expertise. But when such considerations of physical / mental condition are made by others who do not have specific expertise in this area eg an education specialist, then we are more willing to challenge their view – but again, when we have a reasonable basis for doing so.

SAR Information exempt as may cause harm - Health.	DPA	Health	Special rules apply where providing subject accessto information about an individual's physical or mental health orcondition would be likely to cause serious harm to them or toanother person's physical or mental health or condition. These rulesare set out in the Data Protection (Subject Access Modification)(Health) Order 2000 (SI 2000/413), and their effect is to exemptpersonal data of this type from subject access to the extent that itsdisclosure would be likely to cause such harm. To apply this exemption, there clearly needs to be an assessmentof the likelihood of the disclosure causing serious harm. Ifthe data controller is not a health professional as defined in SI 2000/413, the information should not be provided unless the appropriate health professional has been consulted. Section 2 of SI 2000/413 defines the "appropriate health professional" as follows:- (a) the health professional who is currently or was most recently responsible for the clinical care of the data subject in connection with the matters to which the information which is the subject of the request relates; or (b) where there is morethan one such health professional, the health professional who is the most suitable to advise on the matters to which the information which is the subject of the request relates; or (c)wherethere is no health professional available falling within paragraph (a) or (b),a health professional who has the necessary experience and qualifications to advise on the matters to which the information which is the subject of the request relates . The exceptions to the need for a data controller to consult the appropriate health professional are as follows:- 1. where the data controller already has a written opinion from the appropriate health professional obtained within the previous six months that an exemption to the right of subject access exists because the disclosure is likely to cause serious harm to the physical or mental health of the data subject or any other person. However,the data controller may still need to consider whether it is reasonable in all the circumstances to re-consult the health professional before relying on an opinion issued within the previous six months, OR 2. if the individual has already seen or knows about the information concerned. Full legislation available from following link:- http://www.legislation.gov.uk/uksi/2000/413/article/4/made

			A further exemption from subject access to information about anindividual's physical or mental health applies where a SAR is madeby a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointedto manage the affairs of an individual who lacks capacity. In thesecircumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to thatthird party. Full legislation available from following link:- http://www.legislation.gov.uk/uksi/2000/413/article/4/made
SAR Information exempt as may cause harm - Social work	DPA	Health	Special rules apply where providing subject access to informationabout social services and related activities would be likely toprejudice the carrying out of social work by causing serious harmto the physical or mental health or condition of the requester orany other person. These rules are set out in the Data Protection(Subject Access Modification) (Social Work) Order 2000 (SI2000/415). Their effect is to exempt personal data processed forthese purposes from subject access to the extent that its disclosurewould be likely to cause such harm. A further exemption from subject access to social work recordsapplies when a SAR is made by a third party who has a right tomake the request on behalf of the individual, such as the parent ofa child or someone appointed to manage the affairs of an individualwho lacks capacity. In these circumstances, personal data is exemptfrom subject access if the individual has made clear they do notwant it disclosed to that third party.
SAR Information from joint accounts / policies.	DPA	Finance	Generally speaking, if an individual makes a subject access request in relation to a joint account, the individual would be entitled to receive all the personal data relating to that account. This is because joint account holders have equal rights to the account as they are joint (together) and severally (individually) responsible for it. It would follow that the information about the account will be considered to be the personal data of the joint account holders and not restricted to the individual transactions one party has made, as the operation of the account will have an effect on them both. As such, section 7(4) of the DPA would not apply and either of the parties can access the personal data held in the account without the authority of the other. If the account holders together make a subject access request, the data controller would be able to charge each individual £10 whereas if just one of the account holders makes the request, then a maximum of £10 will be charged.

SAR Information in a different language	DPA	Other	- to be intelligible does it have to be translated? Information in a different language can be in an intelligible form but not understandable but the recipient. There is therefore no legal requirement to have the information translated. The key consideration under the Data Protection Act is that individuals are entitled to copies of their personal data in an 'intelligible form'. The act doesn't define 'intelligible form' but our view is that this is reference to information that might not be understandable because – for example – it is in coded format. In such cases we would expect the organisation to provide a key to clarify what the codes mean. Other examples might be handwritten data where it is impossible to decipher the handwriting, in which case we would expect the information to be provided in an intelligible format. Information in a different language can be in an intelligible form but not understandable but the recipient. There is therefore no legal requirement to have the information translated. However, we would say that, as a matter of good practice, some consideration should be given to translating the information to allow the individual to readily access his/her personal data. Obviously, good practice is not the same as a legal obligation.
SAR NHS England - CCGs and CSUs - who is the DC?	DPA	Health	We are receiving a number of enquiries from CSUs about subject access requests they are receiving from patients. CSUs are data processors for NHS England and as such NHS England are the data controller, so all subject access requests should be referred to them. NHS England Email address -england.igqueries@nhs.net

SAR Using S.7 to obtain "Evidence"	DPA	Police, legal & criminal justice	Background This line to take relates to matters where an individual is attempting to obtain evidence for use in support of their position in litigation or when being prosecuted. Such issues are most commonly brought to us as complaints by individuals who have made a subject access request but have not obtained what they required. We may also receive enquiries from data controllers asking if they can refuse to respond to a SAR where the individual is making it purely to obtain documents to assist them in litigation where the individual is making it purely to obtain documents to assist them in litigation. This follows a number of court decisions where the courts have commented that using SARs to obtain documents to assist in litigation is inappropriate and an abuse of process. Line to take The right of subject access is a very powerful right and, apart from the exemptions in Part IV of the DPA, has effect notwithstanding any enactment or rule of law (including court disclosure rules) prohibiting or restricting the disclosure or authorising the withholding of information (s27 (5)).This means that section 7 will have effect unless a data controller can satisfy an exemption from part IV of the DPA. It may be that a subject access request is not always the most appropriate route to obtain information required in connection with legal proceedings, since the right of subject access only entitles individuals to their personal data rather than copies of entire documents or reports. The Criminal and Civil Procedure Rules (CPR) can be a better way of obtaining information required for use in particular litigation or prosecution. Part 31 of CPR provides individuals with an ability to apply to courts asking them to order the disclosure of information the individual requires for the specific purpose of legal proceedings. If the courts have already turned down an individual's requests under CPR, the individual is likely to need to appeal against that decision rather than trying to obtain the information by an alternate route. Confusion has arisen as a result of the previously mentioned comments in a number of court cases, including Durant v Financial Services Authority and Elliot v Lloyds TSB. However, these cases are concerned with the powers of a court in circumstances where an individual seeks to enforce their SAR through the court under section 7(9). It is well established that courts have discretion over whether or not to order disclosure of the disputed personal data. These cases make it clear that, if a court believes that the individual is seeking to use subject access rights to assist in litigation, then they are unlikely to order disclosure. There is more guidance on this in ourSAR code of practice in the section on Exemptions under 'Legal Advice and Proceedings'.

			In any case, section 7(9) does not apply to a data controller who is dealing with the request in the first instance. Section 27(5) makes it clear that they are only entitled to rely on exemptions within part IV of the DPA to withhold information in response to a SAR. As there is no exemption in part IV that allows information to be withheld if the individual is seeking it to assist them with litigation, then they cannot rely on this as a basis for not responding to a SAR.
SAR when the requestor dies during the process	DPA	Other	Occasionally, we receive calls about what should happen in such cases. Provided the requestor was alive when a valid subject access request was received by a Data Controller then they still have to comply with their obligations under the Act. In such cases the response would be sent to the deceased's personal representatives (who would be the people entitled to deal with his estate and who are entitled to his personal information).
Sharing Box Office or ticketing Information	DPA	Direct marketing	Background From time to time the Commissioner receives enquiries regarding the sharing or disclosure of 'box office data'. Generally the enquiries concern the disclosure of details pertaining to individuals who have booked to see a particular production. The problem arises as often those putting on the production are a travelling group who are appearing at various venues. The tickets are booked via the venues and not via the group themselves. E.g. the 'Smith Ballet' company are touring with their production of Swan Lake. They play at various theatres throughout the UK. Tickets are bought via the box offices of the various theatres. The Smith Ballet company, want the theatres to provide them with the contact details of people who have brought tickets so that they can market them with details of forthcoming Smith Ballet Company productions. Line to take Key PointsIf the theatre is a separate data controller from the company performing, and no fair processing information regarding disclosure has been provided by the theatre to the data subjects purchasing tickets, then it is likely that any disclosure of personal data to the Company performing, will be in breach of the Act.Therefore it is important to establish: 1. Who the Data Controller of the data required is. 2. Who requires the data

			3. Whether they are separate Data Controllers. 4. What fair processing information has been provided to data subjects.Even if the disclosure from one Data Controller to another was lawful, and a condition for processing (including the disclosure) was satisfied; the Act would still prohibit the disclosure, unless fair processing information detailing the sharing of data had been provided at the point the data subject contacted the box office. Additional Point It is important to note that even in a situation where disclosure may be compliant with the Act (fair processing info has been provided by the theatre box office to the Data Subject, detailing the disclosure to the theatre company). The theatre company would still need to comply with the Act when conducting their marketing campaign. E.g. Fair processing, lawful, conditions for processing, would need to be satisfied.
Shot gun licenses (certificates) and doctors' records	DPA	Health	There have been a number of questions on the Helpline about the tagging (a separate searchable mark) of medical records for people who are the holders of gun licenses. ACPO are trying to get all the medical records of people who hold a gun license tagged. This is so that if there are any future issues with a patient, the doctor will know they have a gun license and raise this with the police. This tagging would mean that a surgery would know who holds a gun license by doing a search on the specific tag. The ICO has stated that this is disproportionate as any issues about the suitability to hold a gun license would only be with a small number of patients and not all of them. However, the ICO has stated that the letter that is sent to the GP asking about issues relating to the suitability of getting a new gun license or renewing a current gun license can be held on the medical record. This copy of the letter about the suitability for a gun license is on the record, it is not a separate searchable tag.
Smart Meters	DPA	Internet & technology	Energy companies should be open in the information they provide about smart meters; specifically they should provide information about the Data and Communications Company, its role in the system and the regulations and controls that are placed on it. Individuals should be provided with clear information on how the smart metering system will work, including who will have access to data generated by the meter. As the organisations that have the direct relationship with customers, suppliers clearly have a role to play in providing this information. We are currently in discussions with the relevant stakeholders including DECC, Ofgem and Energy UK. We would also mention that the publicity campaign to raise public awareness of smart metering (Smart Energy GB) has now started so we expect public awareness and understanding of the system to increase during 2015.

			What regulations and safeguards are in place in the operation of smart meters pending the roll-out of the system based around the Data and Communications Company, due to come on stream in late 2015? Once the system comes on line in late 2015, organisations operating under licence (eg suppliers, energy networks) will have their access to and use of smart meter data controlled by additional conditions in their licences. Other 'third party' organisations will have their access and use controlled by the Smart Energy Code (SEC). Collectively, these requirements are referred to as the smart meter data access and privacy framework. They will also, of course, have to comply with the relevant legislation, such as the DPA and PECR. In some cases, the framework is actually stricter than the legislation. For example, if organisations wish to use an individual's consumption data (of any granularity) for direct marketing, they must have the explicit consent of the individual first. This is stricter than DPA/PECR, which do not require prior consent in all circumstances. This framework doesn't come in until the rollout begins in 2015. Some suppliers are already fitting what they call 'smart meters'. Our understanding is that, at present, these meters communicate directly with suppliers as the shared infrastructure has not come online yet. The intention is that they will switch over to communicating via the Data Communications Company (Smart DCC Ltd) once the shared infrastructure comes online. The exact technical specifications of a smart meter ('Smart metering equipment technical specifications: second version' or SMETS 2) are not yet finalised. Whilst many of the meters being installed now will be SMETS 2 compliant, some may not. Those that aren't will therefore need to be upgraded or replaced between 2015 and 2020. Ofgem and DECC refer to these non-SMETS 2 compliant meters as 'smart-type' meters for residential properties and 'advanced meters' for non-residential. Ofgem put out aconsultation earlier in the year about extending the privacy framework for smart meters to smart-type and advanced meters. We haveresponded to this, basically saying that we think it would make sense to do so. The consultation is now closed and we are awaiting Ofgem's decision. In the meantime, we would still expect suppliers to comply with the requirements of the DPA when processing any personal data they hold in relation to their customers (including consumption data), just as they would have to with a regular meter. This includes explaining clearly to customers what data they will be collecting and what it will be used for.

Standard letter for EU funded projects approval under FP7	DPA	Other	Standard Letter for EU funded projects approval Your application to the ICO for approval of documents for EU funded projects under FP7 Thank you for your correspondence regarding the above issue in relation your EU funded project. The UK Information Commissioner's office understands that you have requested his approval of documents sent because the FP7 Grant Agreement contains a provision which states: "*The beneficiary(ies) shall provide the Commission with a written confirmation that it has received […] and, **if applicable**, the regulatory approval(s) of the competent national or local authority(ies) in the country in which the research is to be carried out before beginning any Commission approved research requiring such opinions or approvals*." Please accept this letter as confirmation that the ICO does not approve such applications, and therefore is unable to assist you further in this matter.
Surveillance Camera Commissioner (SCC)	DPA	CCTV & optical surveillance	The Protection of Freedoms Act (PoFA) has brought about the appointment of the Surveillance Camera Commissioner (SCC) who has been charged with promoting good practice and encouraging compliance amongst 'relevant authorities' using surveillance cameras. The SCC has produced a new Surveillance Camera Code of Practice (SCCoP). The code sets out 12 guiding principles and provides advice and guidance on issues such as:operational requirements,technical standards, andthe effectiveness of the systems available. The SCC is not concerned with the principles of the Data Protection Act. A 'relevant authority' for the purpose of the SCCoP includes:police,police and crime commissioners,the National Crime Agency, andlocal authorities in England and Wales. Unlike the DPA, the PoFA and therefore the office of the SCC, only applies in England and Wales and does not apply in Scotland or Northern Ireland. Scotland has produced its own CCTV Strategy for Scotland – this strategy sets out the principles that operators of public space CCTV in Scotland must follow.

TPS - Details of the Telephone Preference Service Ltd	PECR	Internet & technology	Background The Telephone Preference Service Limited (TPSL) are the company that run the Telephone Preference Service (TPS), Corporate Telephone Preference Service (CTPS), Fax Preference Service (FPS) and Mailing Preference Service (MPS). TPSL are based in the Direct Marketing Association but actually run these services under contract to Ofcom. Line to take TPSL's responsibilities include maintaining the registers of those 'subscribers that have chosen not to receive unsolicited direct marketing calls. They then make the lists available to marketers so that they can screen against them. They also operate a complaints handling service where they write to companies about the complaints they receive. However they have no powers to enforce the law. The ICO received regular reports from TPSL about the complaints they have received about TPS, CTPS and FPS. Although we do not receive enough information to follow up each complaint again this information helps us to identify persistent offenders and informs our enforcement action.
Universal Jobmatch	DPA	Government - central	Background Following a number of enquiries/concerns which we received regarding the DWP and the new Universal Jobmatch service, we have contacted the DWP to raise concerns about the new online service, particularly in relation to the quality of information about the service, security of the site and contradictory messages about whether it was mandatory or not. We also highlighted to the DWP people's concerns about the wording of the terms and conditions, particularly the disclaimers about who could access people's information, and the lack of clarity about who was the data controller for the online service. What we did Organisations that process personal information are required to do so in accordance with the principles of the Data Protection Act 1998 (DPA). The first data protection principle states that personal data shall be processed 'fairly and lawfully' and a key element of fairness is ensuring people know who is processing their information and how it will be used. We raised our concerns with the DWP and advised that they should review the information they were providing to ensure it complied with the DPA requirements and we recommended that privacy notices should be visible, easy to access and written in a way that could be easily understood by their client group. We also advised of the lack of clarity about which organisation was responsible for the personal data on the Universal Jobmatch online service.

			DWP's response DWP confirmed that the Universal Jobmatch site is a separate, bespoke job search site created for DWP by Monster. It also confirmed that security safeguards had been built into the site but accepted that the disclaimers in the terms and conditions made it appear that this was not the case. DWP informed us that the site was secure and they would look again at the privacy notice and terms and conditions to ensure these complied with the DPA. In response to contradictory information about whether the service was compulsory or not, DWP confirmed on 28 February that Jobseeker Allowance claimants could be required to use the Universal Jobmatch service from 1 March 2013, and that this could well be mandatory. It would appear that to a large extent the enquiries/concerns we have received mainly resulted from unclear information provided through either their websites or staff. We now understand after consulting with the DWP that they have revised the privacy policy, provided additional guidance to advisers, produced leaflets and used easier to understand information about the scheme. We also understand that theterms and conditions have been replaced by a webpage on 'standards of behaviour for jobseekers'. DWP has also assured us that they have taken additional steps to guard against bogus employers, including increased checks on employer and vacancy details. Conclusion We are satisfied that the DWP have taken on board the nature of the concerns and enquiries we have received in relation to Universal Jobmatch and matters of concern with the DPA and that they have put the necessary steps in place to comply with the DPA. If the customer wishes to complain However, it is not within our remit to comment on how this process works or the fact that this has now become a mandatory process. If they have DPA concerns about the process, they need to raise their concerns with the DWP. If they are unhappy with the reply, they can raise a concern with us.
US Surveillance, Snowden and Prism	DPA	Internet & technology	On 7 June 2013 the Guardian ran a story that the National Security Agency in the US was regularly accessing the personal data of UK citizens. The story was published after a secret document was sent to the paper which

			appeared to confirm the details of the secret agreement between the NSA and various companies including Google and Facebook. There are real issues about the extent to which US law enforcement agencies can access personal data of UK and other European citizens. Aspects of US law under which companies can be compelled to provide information to US agencies potentially conflict with European data protection law, including the UK's own Data Protection Act. The ICO has raised this with its European counterparts, and the issue is being considered by the European Commission, who are in discussions with the US Government.
Use of publicly available information	DPA	Internet & technology	Personal data on 'people search' websites A number of websites offer 'people search' facilities providing access to information about individuals from 'public' sources. This can include names, addresses, telephone numbers, and birth and marriage records. Well known websites in this area include 192.com.There are several sets of personal data that other legislation makes available for people to buy or access. This can include information from the electoral roll, records of births and marriages and details of company directors and shareholders. Complying with the DPA - basis for disclosure of information Where other legislation obliges an organisation to make personal data available to the public (for free or for a fee) Section 34 of the DPA provides an exemption allowing them to disclose without breaching the Act. Complying with the DPA – basis for processing An organisation obtaining personal data from one of these legitimate sources and intending to make it available on the internet would still need to satisfy a Schedule 2 condition for their processing. In most cases it is likely they will have to rely on Schedule 2, condition 6 - 'legitimate interests'. This means they would have to balance their legitimate business interests with consideration of whether the way they are using the information could cause unwarranted prejudice to the rights or freedoms or legitimate interests of data subjects. The measures a website could put in place might involve, for example, ensuring there are some restrictions on access and an audit trail by making users register to see records, ensuring there is an option to request removal of records if individuals have personal reasons for objecting, and providing clear information about the source of any data. Individual's rights

			Individuals who object to their information being made available in this way could exercise their rights under the DPA. In particular a Section 10 notice could be used to object to the individual's information being available on the internet on the basis that it was causing substantial, unwarranted damage or substantial, unwarranted distress. If the information is being used for marketing purposes an individual could exercise their Section 11 rights. Complaints If personal information has been obtained legitimately and is processed with consideration for individual's rights in compliance with the DPA the ICO is unlikely to have a basis to prevent sites operating in this way. We could however intervene where there is evidence to suggest individual's rights are not being complied with or the website is making information available in a way that does not comply with other aspects of the DPA.
Vehicle Registration Marks as personal data	DPA	CCTV & optical surveillance	A Vehicle Registration Mark (VRM) is a unique mark linked to a specific vehicle. They can be collected, typically through the use of CCTV and Automatic Number Plate Recognition (ANPR) technology and used for criminal law enforcement purposes or civil matters such as parking enforcement. Where the VRM is collected as part of a system where the ultimate purpose is to identify and take some action against a living individual, such as to serve them with a parking fine, the VRM will be personal data at the point of collection. This is because while the VRM in itself does not identify a living individual, the purpose of the system is such that the data controller is likely to come into possession of further information to enable them to identify either the driver or the registered keeper or both. I Inman 30.04.2014

Win-back campaigns	DPA	Direct marketing	Background This relates to customers who have previously opted out of receiving direct marketing. Line to take When customers have previously opted out to receive direct marketing often data controllers will contact a customer again to see if their preferences have changed. Although the ICO is not opposed to periodically offering customers the chance to opt back in we would expect such letters to accompany correspondence that a customer can reasonably expect to receive. If data controllers write a 'stand alone' letter to an individual asking them to reconsider opting out then this is likely to contravene the Data Protection Act 1998. The worst examples of this kind of breach are when a data controller deliberately opts all of their customers into marketing unless they respond to the correspondence (essentially obtaining consent from a non response).