1.1

Internal Bulletin Online

Sharing FOI knowledge and intelligence

The role of the Data Protection Officer

i
Rate This

Maureen Falconer from the ICO presented on this at the most recent Part 7 Network meeting. Slides are in 83941.

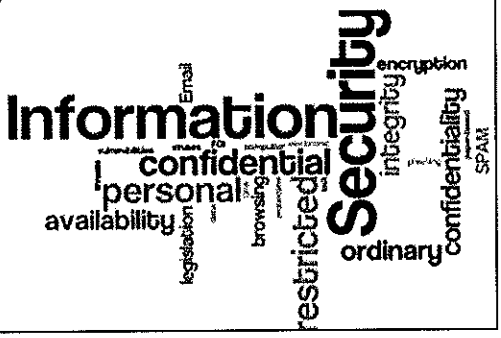
February 15, 2017 - Posted by Paul Mutch | Data Protection, Information Governance, Uncategorized |

No comments yet.

Site info

The role of the Data Protection Officer

Maureen H Falconer
Regional Manager – Scotland
Information Commissioner's Office



Designation of the DPO

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:

1. where the processing is carried out by a public authority or body;

2. where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or

3. where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.

When an organisation designates a DPO on a voluntary basis, the same requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory.

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring. Even though there is no obligation in such cases, the WP29 recommends it as a good practice.

Public Authority or body: Will include national, regional and local authorities and a range of other bodies governed by public law. May include other natural or legal persons governed by public or private law

Core Activities: Primary activity – key operations necessary to achieve the organisations' goals. This is different from 'ancillary functions' such as HR and payroll which, although necessary activity, would not constitute Core Activity

Large Scale: GDPR does not define this but A29WG suggests that consideration be given to: the number of data subjects concerned; the volume of data; the duration or permanence of the data processing activity; the geographical extent of the processing activity. A29WG will publish examples as we go on as indicators of what constitutes large scale.

Expertise & Skills of the DPO

Article 37(5) provides that the DPO be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks set out in Article 39:

Professional qualities:

DPOs should have expertise in national and European DP laws and practices and an in-depth understanding of GDPR. Knowledge of the business sector and organisation is useful and sufficient understanding of the processing, as well as information systems, and data security and data protection needs of the controller. In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

Level of expertise:

This is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data processed. Where processing is complex, or involves a large amount of sensitive data, a higher level of expertise and support is needed. Another factor is whether there are systematic transfers of personal data outside the EU or whether this is occasional. The DPO must be chosen carefully with due regard to the data protection issues that arise within the organisation.

Ability to fulfil tasks:

This includes personal qualities and knowledge but it is also about their position within the organisation. The DPO's primary concern should be enabling compliance with the GDPR and plays a key role in fostering a DP culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches.

Publication of DPO's contact details

Article 37(7) requires the Controller or Processor:

to publish the contact details of the DPO, and

to communicate the contact details to the ICO

This does not mean that the DPO is personally identified!

Contact details should include information allowing individuals and the ICO to reach the DPO in an easy way – post, telephone, email. When appropriate, it might also include a dedicated hotline, or contact form on the website.

This should also apply internally to the organisation via its intranet, internal telephone directory or organisational charts.

Position of the DPO

Article 38 provides that the Controller and Processor shall ensure that the DPO be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

It's crucial that this involvement is at the earliest stage rather than as an afterthought and should include:

- Being invited to participate regularly in meetings of senior and middle management;
- Being present where decisions with DP implications are taken, with all relevant information provided timeously to allow adequate advice to be proffered;
- Due regard given to the DPO's opinion with documented evidence as to why it has not been accepted; and
- Consulted promptly once a data breach or other incident has occurred.

This might be set out in relevant policies and procedures.

Tools to do the job

- Necessary resources (Article 38(2))
- Autonomy and Independence (Article 38(3))
- No fear of dismissal (Article 38(3))
- No conflicts of interest (Article 38(6))

Tasks of the DPO

- Monitoring compliance (Article 39(1)(b))
- PIAs (Articles 35(1) & 39(1)(c))
- Work on a risk-based approach (Article 39(2))
- Record keeping (Articles 30(1&2) 39(1))

Keep in touch

Scotland Office:
45 Melville Street
Edinburgh EH3 7HL
T: 0131 244 9001 E: scotland@ico.org.uk

Subscribe to our e-newsletter at www.ico.org.uk or find us on...

/iconews

@iconews

YouTube LinkedIn

ico.

1.2

Internal Bulletin Online

Sharing FOI knowledge and intelligence

The Role of the DPO

i
Rate This

Act Now blog on the role of the Data Protection Officer, following implementation of the GDPR:

https://actnowtraining.wordpress.com/2017/01/09/gdpr-and-the-role-of-the-data-protection-officer/ (https://href.li/?https://actnowtraining.wordpress.com/2017/01/09/gdpr-and-the-role-of-the-data-protection-officer/)

February 22, 2017 - Posted by Paul Mutch | Data Protection, Uncategorized |

o comments yet.

Site info

GDPR and the Role of the Data Protection Officer

Posted on Monday 9th January 2017

The clock has started on the biggest change to the European data protection regime in 20 years. After four years of negotiation, the new EU General Data Protection Regulation (GDPR) will take effect on 25th May 2018.

In the UK, it will replace the Data Protection Act 1998 (DPA). With some GDPR breaches carrying fines of up to 4% of global annual turnover or 20 million Euros, now is the time to start planning (if you have not already started!).

You might be forgiven for thinking that the Brexit vote means that there is no need to worry about GDPR (being a piece of EU legislation) or that its effect will be time limited. The Government has now confirmed that GDPR is here to stay; well beyond the date when the UK finally leaves the European Union.

Section 4 of GDPR introduces a statutory position of Data Protection Officer (DPO) who will have a key role in ensuring compliance with GDPR. But who exactly will need a DPO and what is his/her role? The Article 29 Data Protection Working Party has now clarified this in its recently published guidance (the A29 Guidance) and a useful FAQ. Technically these documents are still in draft as comments have been invited until the end of January 2017.

Who needs a DPO?

For the first time Data Controllers as well as Data Processors are required to appoint a Data Protection Officer in three situations (Article 37(1)):

1. where the processing is carried out by a public authority or body

Public authorities and bodies are not defined within the legislation. The guidance says that this is a matter for national law. It's fair to say that all bodies subject to the Freedom of Information Act or the Freedom of Information (Scotland) Act will be covered by this requirement e.g. councils, government departments, the health sector, schools, emergency services etc. However it is likely to also cover private companies that carry out public functions or deliver public services in the area of water, transport, energy, housing etc. (See also the decision in Fish Legal v Information Commissioner and others [2015] UKUT 0052 (AAC) which considers the definition of public authorities under the Environmental Information Regulations 2004.)

Purely private companies not involved in public functions or delivering services will only need to appoint DPO if they engage in certain types of data processing operations explained in Article 37:

1. where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale

Under this provision companies whose primary activities involve processing personal data on a large scale for the purposes behavioural advertising, online tracking, fraud prevention, detection of money laundering, administering loyalty programs, running CCTV systems, monitoring smart meters etc. will be caught by the DPO requirement.

c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

The A29 Guidance states that the "and" above should be read to say "or" (a diplomatic way of saying the proof-readers did not do their job!). Special categories of data are broadly the same as Sensitive Personal Data under the Data Protection Act 1998 e.g. ethnic origin, political opinions, religious beliefs, health data etc. This provision will cover, amongst others, polling companies, trade unions and cloud providers storing patient records.

Unless it is obvious, organisations that don't need to appoint a DPO should keep records of their decision making process. The A29 Guidance suggests that it will be still be good practice to appoint a DPO in some cases; for example, where private organisations carry out public tasks. This could include companies delivering core public services under an outsourcing arrangement e.g. housing maintenance companies, charities delivering social services etc. A group of undertakings may appoint a single DPO provided that he/she is easily accessible and there are no conflicts of interests.

Even organisations not based in the EU may be caught by GDPR and the requirement to appoint a DPO. GDPR will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for DP compliance wherever they are based (and not just their EU based offices) as long as they are processing EU citizens' personal data.

The DPO's Tasks

According to Article 37(5), the DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data

Qualities

The A29 Guidance states:

"Although Article 37 does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs should have expertise in national and European data protection laws and practices and an in depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs."

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in depth
- understanding of the GDPR
- understanding of the processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- ability to promote a data protection culture within the organisation

Act Now has recently launched its GDPR Practitioner Certificate aimed at up skilling existing and future DPOs in both the public and private sector. To learn more please visit our website or download the flyer.

The DPO must be allowed to perform tasks in an independent manner and should not receive any instructions regarding the exercise of their tasks. He/She reports to the highest management level in the organisation and cannot be dismissed or penalised for doing their job.

Article 38(2) of GDPR requires the organisation to support its DPO by "providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge." The A29 Guidance says that, depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Active support of the DPO's function by senior management
- Sufficient time to for DPOs to fulfil their duties
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- Official communication of the designation of the DPO to all staff
- Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- Continuous training

The DPO will be at the heart of the data protection framework for many organisations, facilitating compliance with the provisions of the GDPR. Now is the time to appoint one to ensure that you get the most suitably qualified. Some say 28,000 will be required in the UK and US. Others have even suggested there will be a skills shortage!

There is certainly a lot to learn and do in less than 18 months when GDPR comes into force. Training and awareness at all levels needs to start now.

Do you think mandatory Data Protection Officers under GDPR will lead to higher salaries for DPOs?

Participate in our Twitter survey:

Make 2017 the year you get prepared for the General Data Protection Regulation (GDPR). See our full day workshops and new GDPR Practitioner Certificate.

Share this:

Press This Twitter LinkedIn

Reblog Like

One blogger likes this.

About actnowtraining

Act Now Training Ltd specialise in information law. We have been providing training and consultancy services globally for over 15 years. We have an extensive GDPR course programme from live and recorded webinars, accredited foundation through to higher level certificate courses delivered throughout the country or at your premises. We pride ourselves on having well renowned experts in the fields of Data Protection, Freedom of Information, Surveillance Law and Information Management. All our experts have worked within the public and private sectors and have many years of experience of training and consulting in these areas. Our clients include central government, local authorities, multi-national corporations as well as other public and third sector bodies including schools. Please visit our website to see the range and testimonials of our satisfied clients.
View all posts by actnowtraining →

This entry was posted in Certificated course, Data Protection, DPO, EU DP Regulation, GDPR and tagged DPO. Bookmark the permalink.

17 Responses to *GDPR and the Role of the Data Protection Officer*

Pingback: *The Subject Access Under GDPR | Blog Now*

Pingback: *ICO Local Government Survey: Councils trying to Get Ready for GDPR | Blog Now*

Pingback: *GDPR Guidance finalised and more published | Blog Now*

Pingback: *GDPR Practitioner Certificate: First set of Results | Blog Now*

Pingback: *Data Protection Impact Assessments under GDPR | Blog Now*

Pingback: *GDPR and Employee Surveillance | Blog Now*

Pingback: *The Data Protection Bill: A Summary | Blog Now*

Pingback: *GDPR Practitioner Certificate: Another Set of Great Results | Blog Now*

Pingback: *GDPR Practitioner Certificate: New Course For Manchester | Blog Now*

Pingback: *Act Now Launches GDPR Handbook | Blog Now*

Pingback: *GDPR: Updating Privacy Notices | Blog Now*

Pingback: *GDPR is coming but don't panic! | Blog Now*

Pingback: *GDPR and Data Protection Impact Assessments: When and How? | Blog Now*

Pingback: *The Data Protection Act 2018: A Summary | Blog Now*

Pingback: *ICO Refuses to Disclose GDPR Policy Document for Special Categories Data | Blog Now*

Pingback: *GDPR: What Will the Data Protection Officer Role Look Like? - Recruitment Revolution*

Pingback: *GDPR Practitioner Certificate: New Course For London | Blog Now*

Blog Now

Blog at WordPress.com.

1.3

Internal Bulletin Online

Sharing FOI knowledge and intelligence

GDPR preparations – update from Helen

i
Rate This

GDPR preparations – update

As you know, data protection requirements are changing from 25 May 2018 when the General Data Protection Regulation (GDPR) comes into force and the Data Protection Bill is also due to come into force.

GDPR Implementation Plan 2018-19 (VC100858)

` new plan is in place for 2018-19 and the GDPR Working Party (HGS,MK,EM,LC,LB) is now meeting weekly to ensure that we comply with the new requirements. The areas that the Working Party are currently working on include:

- Personal data audit – evaluation and actions
- Privacy notice/s
- Subject access
- Consent
- Human resources and employment records
- Law enforcement
- Liaison with IT services providers (Microsys, CAS, C2 Software) and payroll and pension providers
- Procurement and contract requirements
- Cyber security

A number of our policies and procedures are being updated and you will be notified of these as the work progresses.

Myself and Euan McCulloch are also representatives on the Scottish Parliamentary Corporate Body (SPCB) GDPR Working party (monthly meetings).

Data Protection Officer (DPO)

The SPCB has proposed a shared service DPO for Officeholders and we have provided comments on the draft MOU. I will let you know when a DPO has been appointed.

Training

GDPR training was provided to staff last year and further training on "Data Protection Reform: Can we have the Bill please": by David Freeland, ICO (VC97644) and "The new data protection rules and FOI" by Margaret Keyse (VC97528) was provided on 16 January 2018.

Training is being provided by Act Now tomorrow (17 April 2018) – the course outline is attached to the calendar invite which has been sent to all staff.

The SPCB has also offered to let us link into its online GDPR training – this is being tested at present and I will let you know when this is due to be rolled out to us.

If you have any questions or comments please speak to me or a member of the GDPR Working Party.

Helen

April 16, 2018 - Posted by Liz Brown | Data Protection |

No comments yet.

Site info

1.4

The GDPR Working Party (myself, Margaret, Euan, Lorraine and Liz) meets approx. every 2 weeks – matters considered include the progress of the Data Protection Bill, the latest guidance from the Article 29 Working Party and the ICO (see VC 96629), the Compliance Plan (VC83922) and the preparations/actions needed to ensure that SIC will comply with the GDPR when it comes into force in May 2018. The areas we are currently working on are:

- Personal data audit – being carried out in teams and Working Party will assess the results – relevant documents are: the guidance on completing the audit can be found in VC94032
- Liaison with IT services providers (Microsys, CAS, C2 Software) and payroll and pension providers re: re: GDPR Supplier Checklist (VC96619)
- Privacy notices
- Subject access
- Procurement – relevant issues to be considered
- Privacy and Electronic Communications Directive (PECR) and impact

The GDPR Working Party Agenda & Actions can be found in VC89498.

Myself and Euan are also representatives on the SPCB GDPR Working party (monthly meetings) which enables us to have an input into the actions being taken by Officeholders as regards GDPR preparation and compliance. The SPCB is currently considering a shared service proposal for a Data Protection Officer (with possible team) for Officeholders and we are awaiting final details of the proposal.

All staff received GDPR training last year and further training is being arranged to take place in the last two weeks in April 2018. The training dates are being finalised and will be provided as soon as possible.

If you have any questions or would like any further information about our preparations for the implementation of the GDPR on 25 May 2018 please let me know.

2.1

Committee Report

ITEM 20

Report to:	QSMTM
Report by:	Helen Gardner-Swift
Meeting Date:	31 January 2018
Subject/ Title: (and VC no)	**GDPR Update** **VC98207**
Attached Papers (title and VC no)	SIC Implementation/Compliance Plan VC83922

Purpose of report

1. To update the Senior Management Team (SMT) on the implementation of the General Data Protection Regulations (GDPR) requirements.

Recommendation and actions

2. The SMT notes the contents of this report; and
3. The SMT agrees that the SIC appoint a DPO, as required by the GDPR.

Executive summary

[redacted]

[redacted]

DPO

12. We are a public authority and, under the GDPR, we are required to appoint a DPO.

13. The DPO's minimum tasks are defined in Article 39 of the GDPR and include:
    (i) To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
    (ii) To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
    (iii) To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

14. The GDPR does not specify the precise credentials a data protection officer is expected to have but it does require that they should have professional experience and knowledge of data protection law - this should be proportionate to the type of processing we carry out, taking into consideration the level of protection the personal data requires.

15. As regards the appointment of a DPO, we must ensure that:

    (i) the DPO reports to the highest management level, that is the SMT; and
    (ii) the DPO operates independently and is not dismissed or penalised for performing their task; and
    (iii) adequate resources are provided to enable the DPO to meet their GDPR obligations.

16. The role of the DPO can be allocated to an employee as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. The role of the DPO can also be contracted out externally. A single DPO can also be appointed to act for a group of public authorities, taking into account their structure and size.

17. As yet, the SPCB have not confirmed the details of the shared service proposal concerning the appointment of a DPO for Officeholders. However, at a meeting of the SPCB GDPR Working Party on 25 January 2018, it was indicated that the DPO to be appointed under the shared service proposal is likely to be an employee of the SPCB. The SIC raised concerns about this as regards confidentiality and conflict of interests. We are awaiting further details

about the proposal, including confirmation as to whether it is intended to be an employee of the SPCB.

18. As it is likely that the shared service proposal may not be suitable for the SIC, I propose that we seek to appoint our own DPO.

[redacted]

[redacted]

Committee Report 2.2

ITEM 26

Report to:	QSMTM
Report by:	Helen Gardner-Swift
Meeting Date:	25 April 2018
Subject/ Title: (and VC no)	**GDPR Update** **VC101275**
Attached Papers (title and VC no)	GDPR Implementation Plan 2018-19 VC100858

Purpose of report

1. To update the Senior Management Team (SMT) on the implementation of the General Data Protection Regulation (GDPR) requirements.

[redacted]

[redacted]

[redacted]

Data Protection Officer (DPO)

10. We are a public authority and, under the GDPR, are required to appoint a DPO. The DPO's minimum tasks are defined in Article 39 of the GDPR and include:

    - To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
    - To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
    - To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

11. The GDPR does not specify the precise credentials a DPO is expected to have but it does require that they should have professional experience and knowledge of data protection law - this should be proportionate to the type of processing we carry out, taking into consideration the level of protection the personal data requires.

12. As regards the appointment of a DPO, we must ensure that:

    - the DPO reports to the highest management level, that is the SMT; and
    - the DPO operates independently and is not dismissed or penalised for performing their task; and
    - adequate resources are provided to enable the DPO to meet their GDPR obligations.

13. The role of the DPO can be allocated to an employee as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. The role of the DPO can also be contracted out externally. A single DPO can also be appointed to act for a group of public authorities, taking into account their structure and size.

14. The SPCB has put forward a shared service proposal for a DPO for Officeholders and we have provided comments on the draft MOU and are awaiting a response from the SPCB.

15. In the event that we enter into the proposed MOU and, subsequently, there is a conflict of interest which means that the SPCB DPO cannot act for the SIC, it is anticipated that a Deputy Head of Enforcement will act as a DPO (only in in these circumstances).

[redacted]

Committee Report 2.7

Report to:	QSMTM
Report by:	Helen Gardner-Swift
Meeting Date:	1 June 2018
Subject/ Title: (and VC no)	**GDPR Update** **VC103002**
Attached Papers (title and VC no)	The GDPR Implementation Plan 2018-19 VC100858

Purpose of report

1. To update the Senior Management Team (SMT) on the implementation of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 requirements.

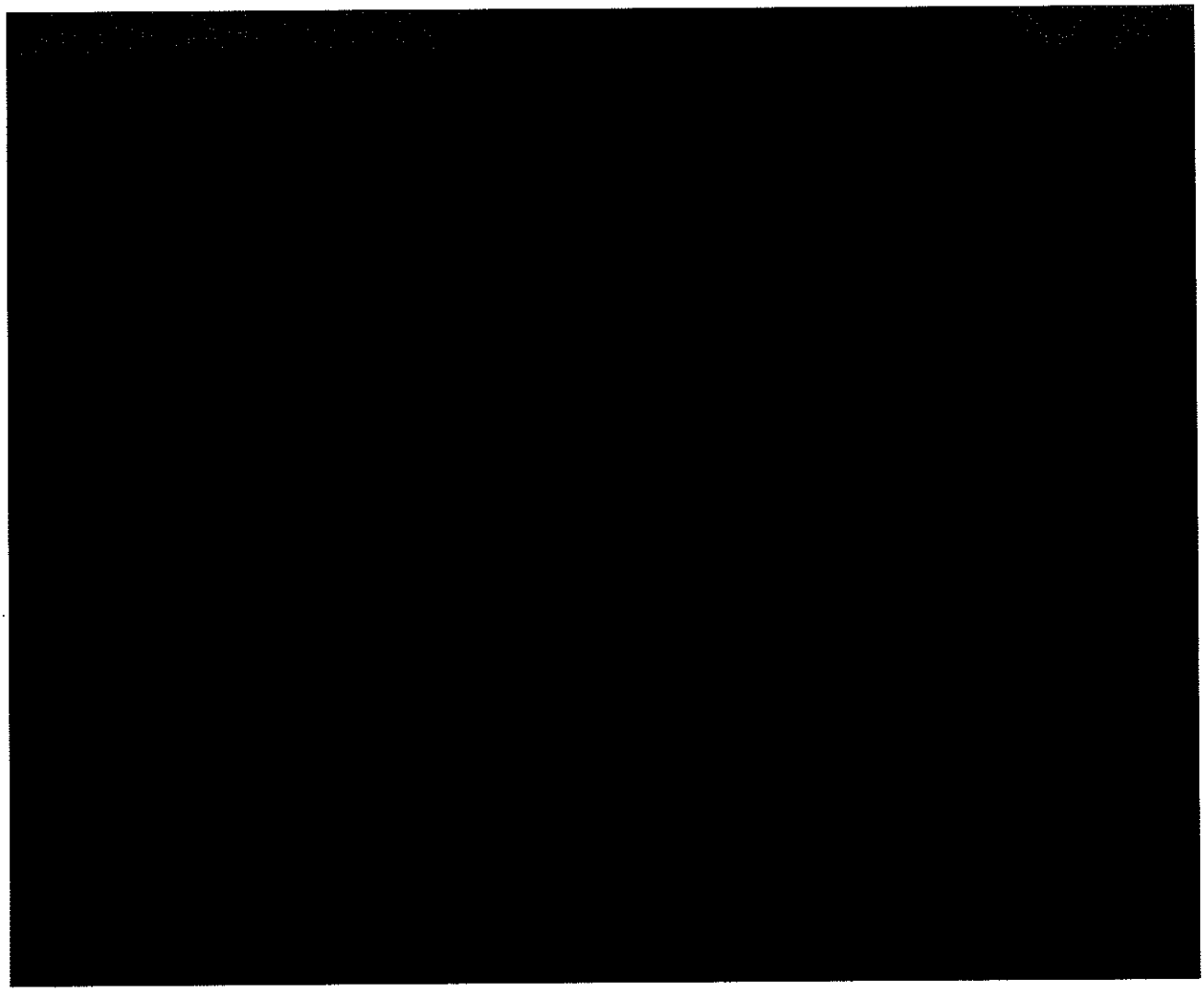
[redacted]

[redacted]

Data Protection Officer (DPO)

9. The SPCB has provided a shared DPO service and the MOU for this was signed on 24 May 2018. Euan McCulloch has agreed to act as DPO if a conflict of interests arises in the operation of the shared service DPO.

[redacted]



3.1

Scottish Information Commissioner

Minutes of the Additional Quarterly Senior Management Team Meeting

01 June 2018

NOTE TO READER:
The Scottish Information Commissioner publishes the minutes of Quarterly Senior Management Team (SMT) meetings and the papers considered at the meetings, unless he considers, at the time of publication, that the minutes and/or papers are exempt from disclosure under the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004 (FOI law). Where minutes or documents are not published, the minutes will make it clear why not.

Under FOI law, everyone has the right to request any information held by the Commissioner. This includes minutes or papers which have not been published. If you want to request copies of minutes or documents which haven't been published, make a request (in writing, by e-mail or in any other recordable form) to:

Scottish Information Commissioner, Kinburn Castle, Doubledykes Rd, St Andrews, Fife, KY16 9DS
Tel 01334 464610
Fax 01334 464611
enquiries@itspublicknowledge.info

Present: Daren Fitzhenry (DF), Margaret Keyse (MK), Sarah Hutchison (SH), Helen Gardner-Swift (HGS), Liz Brown (LB) (Minutes)

Details	Action By	Target Completion Date	Publish Yes / No	Comments
[redacted]				

[redacted]

6. GDPR - Implementation

• The report was noted • The arrangements in place for EM to act as DPO if a conflict of interest arises in the operation of the shared service DPO need to be documented	HGS	30/06/18		Committee Report published in full Background papers not published – exemption s30(b)(ii) s39(1)

[redacted]

Signed off by:

Date: 18 June 2018

Agreed 4.1

Minutes of Meeting: GDPR – Data Protection Officer

First meeting - 8 June 2017 at 2.30pm at the Scottish Parliament

Attendees: Bill Thomson, ESC
Karen Elder, ESC
Val Malloch, SPSO
Helen Littlemore, SPSO,
Stephen Grounds, CYPCS
Gillian Munro, CYPCS
Clare Nicolson, SHRC
Elaine McLean, SCS
Helen Gardner-Swift, SIC
Euan McCulloch, SIC
Clare Turnbull, SP
Isla Mcleod, SP
David Birrell, SP
Robert Black, SP
Janice Crerar, SP

Introductions

1. Janice Crerar welcomed everyone to the meeting and outlined that the purpose of the meeting was to provide a brief update on GDPR developments and to discuss the role of the DPO and in particular whether there could be scope for the SPCB's DPO (once appointed) to be offered to officeholders on a shared services basis although it was stressed that no decision had been made on whether this would be possible.

[redacted]

Open Discussion

3. Matters arising from the open discussion included the following:-

[redacted]

- DPO needs to be in place as soon as possible;
- It may be possible to share the SPCB's DPO (if this could be offered on a shared service basis) but subject to SLA's being drafted and agreed

2d page?

4.2

Minutes of Meeting: GDPR – Data Protection Officer

Second meeting - 27 June 2017 at 11am at the Scottish Parliament

Attendees: Bill Thomson, ESC
Val Malloch, SPSO
Stephen Grounds, CYPCS
Gillian Munro, CYPCS
Sharon Barbour, SHRC
Elaine McLean, SCS
Helen Gardner-Swift, SIC
Clare Turnbull, SP
Isla Mcleod, SP
Janice Crerar, SP

Apologies: Helen Littlemore, SPSO
Euan McCulloch, SIC
Karen Elder, ESC

[redacted]

[redacted]

SPCB's DPO

5. The group was given an update on the initial steps being undertaken by the GDPR Project in terms of the requirement for the Parliament to appoint a DPO. A detailed job description has been drafted and will be shared with the group. On timing, a paper is planned to go to the SPCB in early September on the implications of GDPR and the appointment of a DPO and whether the DPO can be offered to the officeholders on a shared service basis.

6. As we will not have a decision in time for the submission of budget bids, it was suggested that officeholders should make provision in their budget bids for a DPO.

Other Matters

7. A number of other matters were raised including:-

[redacted]

- Whether one shared DPO would be sufficient; and
- Managing conflicts of interest.

Service Level Agreement (SLA)

8. The subject of an SLA came up and the group agreed this was key to determining whether a shared DPO would be possible. Helen offered to draft an SLA but asked the other offices to provide her with comments on what should be

included. Helen agreed to provide a draft by end July so any comments should be sent to Helen in good time to allow her to incorporate them.

Next Meeting

9. The next meeting will be on Tuesday 1 August at 11.30am at the Scottish Parliament.

Janice Crerar
Officeholder Services
3 July 2017

4.3

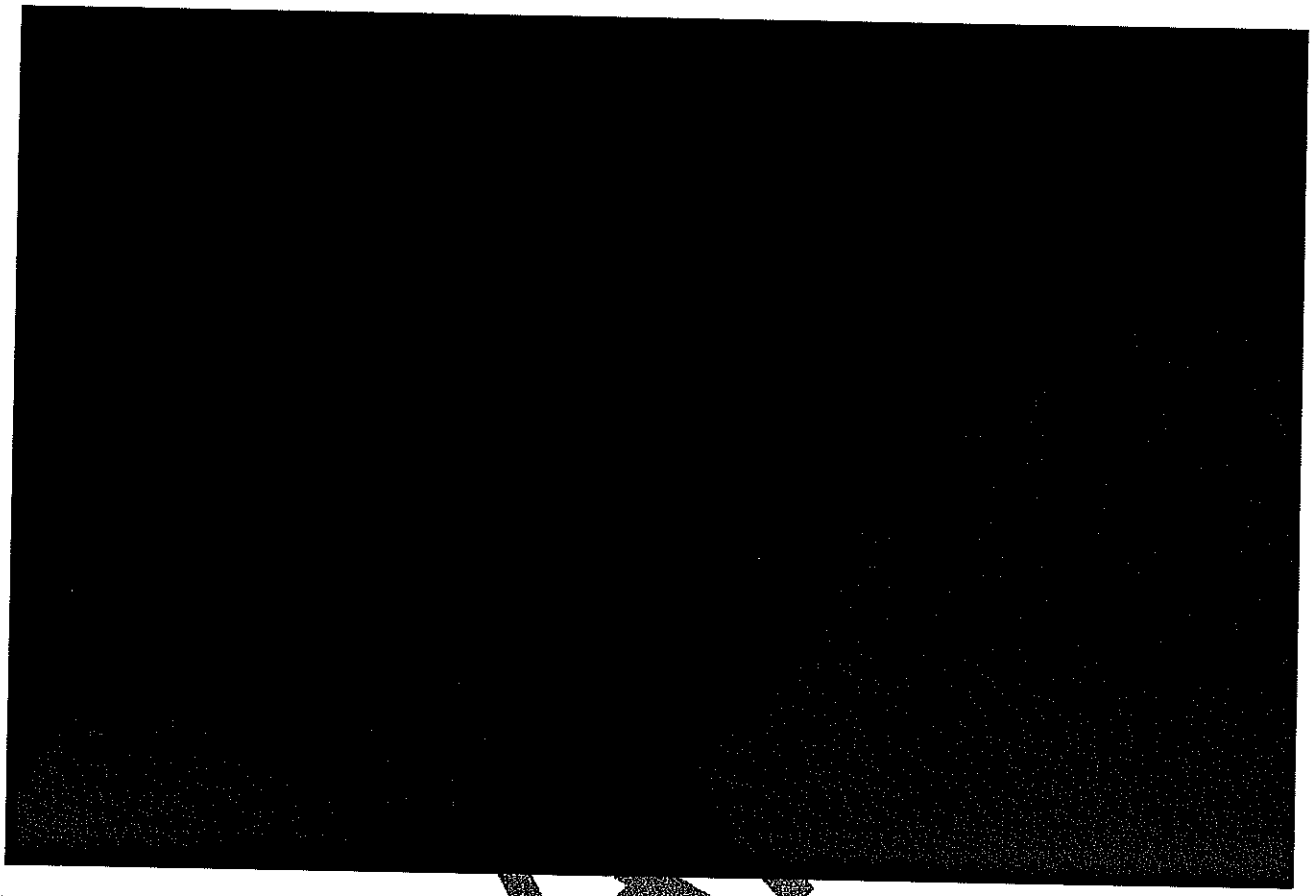
Minutes of Meeting: GDPR – Data Protection Officer

Third meeting – 1 August 2017 at 11.30am at the Scottish Parliament

Attendees: Euan McCulloch, SIC
Helen Gardner-Swift, SIC
Val Malloch, SPSO
Gillian Munro, CYPCS
Stephen Grounds, CYPCS
Elaine McLean, SCS
Karen Elder, ESC
Clare Nicolson, SHRC
Sharon Barbour, SHRC
Clare Turnbull, SP
David Birrell, SP
Janice Crerar, SP

Apologies: Helen Littlemore, SPSO
Isla Mcleod, SP

[redacted]



DPO Draft Specification – paper from Helen Gardner-Swift

4. Helen was thanked for drafting and circulating her draft specification of requirements for the provision of a DPO to the officeholders. Helen invited written comments on the draft by **25 August**. Comments should be sent to hgardnerswift@itspublicknowledge.info, copied to the other members of the group.

5. Janice reminded the group that there continued to be options with regard to the provision of a DPO including

   (i) outsourced via a contract;
   (ii) out-sourced via a shared contract between the SPCB and the officeholders; and
   (iii) the SPCB would provide a DPO at nil cost to the officeholders, if this was possible and parties were agreeable.

Next Meeting

6. The next meeting will be on Monday 11 September at 2pm at the Scottish Parliament.

Janice Crerar
Officeholder Services

4.4

Minutes of Meeting: GDPR – Data Protection Officer

4th Meeting – 11 September 2017 at 2pm at the Scottish Parliament

Attendees: Helen Gardner-Swift, SIC
Val Malloch, SPSO
Gillian Munro, CYPCS
Stephen Grounds, CYPCS
Elaine McLean , SCS
Ruth Hogg, ESC
Isla Mcleod, SP
Janice Crerar, SP

Apologies: Helen Littlemore, SPSO
Clare Nicolson, SHRC
Sharon Barbour, SHRC
Claire Turnbull, SP

[redacted]

[redacted]

[redacted]

Information Governance/Data Protection Specialist – paper from Gillian Munro

5. The group thanked Gillian for her paper and noted that choices were limited resulting in there not being a lot of information available on costs etc. Helen mentioned that she had spoken to SIC's internal auditors (Scott Moncrieff) re the possibility of auditors providing a GDPR service. Although nothing was in place Scott Moncrieff considered that firms would be looking at whether this was something that they could provide.

DPO Draft Specification – paper from Helen Gardner-Swift

6. It was agreed that the discussion on Helen's paper be postponed until the next meeting to give members more time to consider and give Helen comments and to allow for an in-depth discussion.

[redacted]

Janice Crerar, Officeholder Services

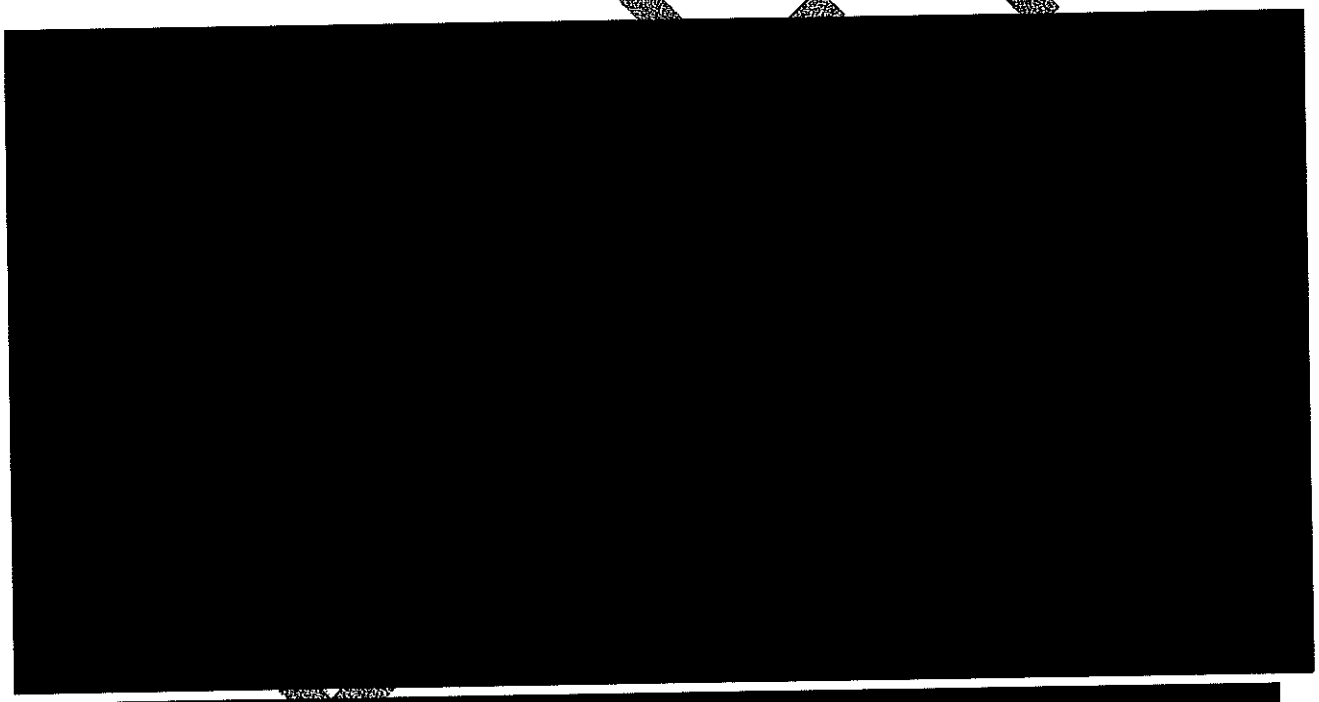
4.5

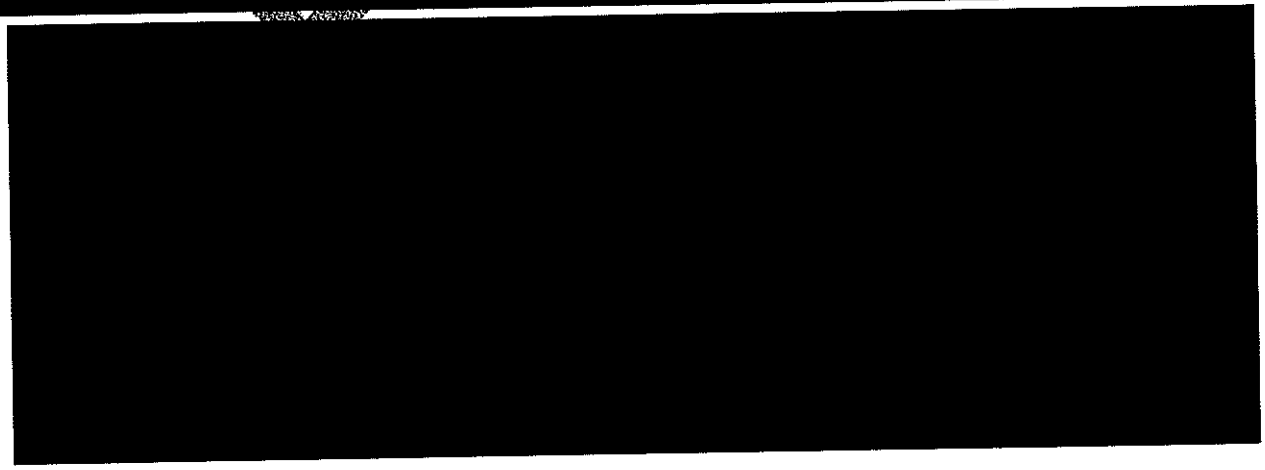
Minutes of Meeting: GDPR – Data Protection Officer

5th Meeting – 12 October 2017 at 10am at the Scottish Parliament

Attendees: Helen Gardner-Swift, SIC
Euan McCulloch, SIC
Helen Littlemore, SPSO
Gillian Munro, CYPCS
Stephen Grounds, CYPCS
Claire Turnbull, SP
Isla Mcleod, SP
Janice Crerar, SP

Apologies: Karen Elder, ESC
Val Malloch, SPSO
Clare Nicolson, SHRC
Sharon Barbour, SHRC





[redacted]

DPO Draft Specification – paper from Helen Gardner Swift

4. Helen summarised the comments received from the officeholders and there was then a general discussion on all the points made. On next steps, JC suggested that she would convert the document to a draft MOU and would circulate it for comment. The group thanked Helen for preparing the document.

[redacted]

Janice Cridlan
Officeholder Service

4.6

Minutes of Meeting: GDPR – Data Protection Officer

6th Meeting – 17 November 2017 at 10.30am at the Scottish Parliament

Attendees: Karen Elder, ESC
Helen Gardner-Swift, SIC
Helen Littlemore, SPSO
Gillian Munro, CYPCS
Sharon Barbour, SHRC
Janice Crerar, SP

Apologies: Val Malloch, SPSO
Clare Nicolson, SHRC
Euan McCulloch, SIC
Stephen Grounds, CYPCS
Claire Turnbull, SP
Isla Mcleod, SP

[redacted]

[redacted]

[redacted]

- Janice gave an update for the SPCB in Claire's absence. [redacted]

[redacted] The issue of appointing a DPO will be considered thereafter. Helen (G-S) asked if it would be possible to know by January 2018 if the SPCB's DPO could be a shared service. Janice gave a commitment to let the officeholders know as soon as possible what the SPCB's plan is in that regard.

[redacted]

Janice Crerar
Officeholder Services
November 2017

S.1

Margaret Keyse

From: David Lowrie
Sent: 07 February 2017 15:56
To: 'Crerar J (Janice)'
Subject: RE: GDPR and Data Protection Officer (DPO)

Thanks Janice

From: Crerar J (Janice) [mailto:Janice.Crerar@parliament.scot]
Sent: 07 February 2017 15:52
To: Clare C. Nicolson; David Lowrie; McLean El (Elaine); Karen K. Elder; Fiona F. Paterson; Stephen S. Grounds
Subject: GDPR and Data Protection Officer (DPO)

Dear All

Just a quick update to let you know that we are currently considering the impact of the GDPR and in particular the role and designation of Data Protection Officers and hope to be able to let you have an update in March.

Kind regards

Janice

The Scottish Parliament
Pàrlamaid na h-Alba
Mrs Janice Crerar
Officeholder Services
The Scottish Parliament
Edinburgh
EH99 1SP
Telephone: 0131 348 6851
email – janice.crerar@parliament.scot

J.2

Legal Advice

Scottish Information Commissioner

To	Rosemary Agnew	**Date**	28 March 2017
cc.			
From	Margaret Keyse		
Subject	**Legal Advice: Data Protection Officers' Independence under the GDPR**		

1. This is in response to your email of 24 March 2017, the text of which is copied below.

2. During the presentation, Fiona Killen said, in response to a question, that "conflict of interest will be a real issue for the Commissioner" and that, in her view, we would not be able to share a DPO with another data controller.

3. The section in quotes is from my notes on the slide. The other part is from memory. We do not have any additional notes from Anderson Strathern in addition to the slides they gave us (saved in VC82228).

4. Article 37(1)(a) of the GDPR requires all public authorities to designate a DPO. Article 37(3) states that a single DPO may be designated for several public authorities taking account of their organisational structure and size.

5. Article 38(1)(6) contains a reference to "conflict of interests", but the focus there is on the other tasks and duties the DPO may be asked to fulfil (i.e. tasks unconnected with the role of the DPO) and does not focus on a conflict of interests a DPO may face in acting for more than one public authority.

6. I checked the guidelines issued by the Article 29 Working Group on 13 December 2016 on DPOs here. There is nothing specifically in the guidelines which suggest that, for data controllers such as us, we can't share a DPO with another data controller. The focus in the guidelines (as well as in the GDPR) is on making sure, taking account of organisational structure and size, that a single DPO can perform their tasks efficiently, despite being responsible for several public authorities. We also need to make sure that the DPO is personally available when we need them – either physically, via a hotline or other secure means of communication.

7. It's also useful to note that DPOs will be bound by secrecy or confidentiality concerning their performance of their tasks, in accordance with EU or Member State law (Article 38(5)). Therefore, despite their "independence", the DPO will remain subject to section 45 of FOISA for all work done on behalf of the Commissioner and disclosure will be a criminal offence unless done with lawful authority.

8. Given the wording of the GDPR and the guidelines, I don't have the same concerns that Fiona does over a conflict of interests. I can understand that there might be some disquiet about us sharing a DPO with the bodies we regulate (and, at least in the case of the SPSO, with bodies which regulate us). However, the focus of the DPO is on data governance as a

whole, rather than on decisions to be taken by the Commissioner in response to applications made under FOISA or the EIRs and that is where I see the conflict of interest would come in..

9. I see no reason why, particularly in the light of section 45 of FOISA, we couldn't draw up an agreement which designed to avoid conflict of interests while allowing the DPO to carry out their full tasks under the GDPR.

Margaret

When I met with SPCB on Monday, we discussed briefly the role of the Data Protection Officer. SPCB are currently looking at this for the Parliament and in respect of office holders. In respect of the office holders they were considering providing this as a shared service. I told them that my understanding from the training from AS was that it could not be a shared service for us because of the conflict of interest. I recalled this being the verbal advice given when we received the AS training (attached for information). I said I would send them the slides.

Before doing so I reviewed them and realise that read on face value, they support the approach

SPCP is considering.

Is there an additional note anywhere of the advice AS gave us? If not could you do me an internal legal advice note, making reference to the AS presentation that I could share with SPCB.

I'm not expecting a response today, but sometime next week would be really helpful.

Thanks

Rosemary

Rosemary Agnew
Scottish Information Commissioner

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: ragnew@itspublicknowledge.info
Web: www.itspublicknowledge.info

Scottish Information Commissioner
it's public knowledge

Helen Gardner-Swift

From: Rosemary Agnew
Sent: 06 April 2017 17:03
To: Jann Wallace
Cc: Margaret Keyse; Helen Gardner-Swift
Subject: FW: GDPR - Data Protection Officer
Attachments: Info for officeholders re GDPR 2017.03.27.docx

In Virtual Cabinet: 0

Thanks Jann

Leave it with me. I would like to discuss this at WSMTM before we agree to anything, including the date and who attends the meeting.

Rosemary Agnew
Scottish Information Commissioner

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: ragnew@itspublicknowledge.info
Web: www.itspublicknowledge.info

Scottish Information Commissioner
it's public knowledge

From: Jann Wallace
Sent: 06 April 2017 16:58
To: Rosemary Agnew; Margaret Keyse; Helen Gardner-Swift
Subject: FW: GDPR - Data Protection Officer

Hello,

Rosemary/Margaret, you may already be on the DPO case. Please see Janice's email below.

Thanks
Jann

From: Crerar J (Janice) [mailto:Janice.Crerar@parliament.scot]
Sent: 06 April 2017 15:04
To: Karen K. Elder; Stephen Grounds; Helen.Littlemore@spso.gsi.gov.uk; McLean El (Elaine); Clare C. Nicolson; Jann Wallace
Cc: Turnbull CM (Claire)
Subject: **SPAM** GDPR - Data Protection Officer

Dear All

As you are all aware, under the GDPR there is a requirement for organisations to designate a DPO with effect from 25 May 2018. We have been considering whether there is scope for the SPCB to offer this as a shared service or through a contract to which the officeholders would have access to.

To progress matters we intend to hold a meeting on 8 June at 2.30pm at the Parliament and I would be grateful if you could confirm if that date and time is suitable for you.

In the meantime, I attach a draft person specification and job role for the new DPO role (which is based entirely on the guidance from the Article 29 Data Protection Working Party) and I would be grateful for your comments. It would also be helpful if you could quantify the volume of personal data that your respective offices process to enable us to estimate the overall requirement.

If I should have sent the email to another colleague in your organisation, please let me know

Kind regards

Janice.

Mrs Janice Crerar
Officeholder Services
The Scottish Parliament
Edinburgh
EH99 1SP
Telephone: 0131 348 6851
email – janice.crerar@parliament.scot

General Data Protection Regulation (GDPR)

The GDPR provisions come into force on 25 May 2018

The GDPR will provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPO's) will be central to the new legal framework for facilitating compliance with the provisions of the GDPR. The GDPR lays down conditions for the appointment, position and tasks of a DPO.

Under the GDPR, it is mandatory for public authorities to designate a DPO.

The Article 29 Working Group (an independent advisory body on data protection and privacy was established under Article 29 of Directive 95/46/EC) has produced guidance which was adopted on 13 December 2016. On the basis of this guidance we have drawn up a draft job role and person specification which is attached at Annex A.

In considering the role the following should be taken into account:-

Accessibility:

The DPO, internal or external, must be accessible and available to communicate with the data processor or controller and with data subjects. Given this, DPOs must be easy to access and their contact details must be made public.

Resources:

Article 38(2) requires organisations to support the DPO "*by providing resources necessary to carry out [their] tasks and access to personal data and processing operations and to maintain his or her expert knowledge*".

The Article 29 Working Group identifies that depending on the nature of the processing operations, and the activities and size of the organisation, the following resources should be provided for the DPO:

- Active support of the DPO's function by senior management;
- Sufficient time for the DPOs to fulfil their duties;
- Adequate support in terms of financial resources, infrastructure(premises, facilities, equipment) and staff where appropriate;
- Official communication of the designation of the DPO to all staff;
- Access to other services within the organisation so that the DPO(s) can receive essential support, input or information from those other services; and
- Continuous training

Conflict of Interest:

The guidance provides that the DPO can undertake other tasks and duties as long as they do not constitute a conflict of interest.

The absence of any conflict of interest is closely linked to the requirement for the DPO to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to a conflict of interest. In particular the DPO cannot hold a position in the organisation that leads him or her to determine the purposes and the means of processing personal data. This requirement is to be considered on a case by case basis depending on the specific structure within an organisation.

Conflicting positions may include senior management such as the Chief Executive, the Chief Financial or Operating Officer, the Head of Marketing, the Head of Human Resources, or head of IT departments, and also lower down the organisational structure if such positions or roles lead to determination or purposes and means of processing.

Autonomy:

Article 38(3) establishes some basic guarantees to ensure that the DPOs are able to perform their tasks with a sufficient degree of autonomy within an organisation. In particular controllers and processors are required to ensure that the DPO "does not receive any instructions regarding the exercise of [his or her] tasks. Recital 97 adds that DPOs "*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.*"

Article 38(3) requires the DPO to report directly to the highest management level of the organization.

Article 38(6) allows DPOs to "*fulfil other tasks and duties*", but notes that the organisation should ensure that "*any such tasks and duties do not result in a conflict of interest.*"

ANNEX A

DPO Role and person specification

The DPO's primary concern should be enabling compliance with the GDPR. It is crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection. Ensuring the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, ensure a privacy by design approach and should therefore be standard procedure with the organisation's governance structure. It is important that the DPO is seen as a discussion partner and part of any relevant working groups dealing with data processing activities.

The DPO should be for example:-

- invited to participate regularly in meetings of senior and middle management;
- invited to meetings where decisions with data protection implications are taken. All relevant information must be passed to the DPO in a timely manner in order to allow the DPO to provide adequate advice;
- their opinion must always be given due weight. Where their advice is not taken this should be documented; and.
- they must be promptly consulted once a data breach or incident has occurred.

Key Tasks:

Article 39(1)(b) highlights that the DPO has a duty to monitor compliance with the GDPR. Recital 97 further specifies that the DPO "*should assist the controller or the processor to monitor internal compliance with this Regulation.*"

Monitoring duties may include:

- Collecting information to identify processing activities
- awareness-raising, and training of staff involved in the processing operations, and the related audits
- to provide advice where required as regards the data protection impact assessment and monitor its performance in line with Article 35
- to co-operate with the supervisory authority (ICO in the UK)
- Analysis and checking of compliance of processing activities
- to act as the contact point for the supervisory authority on issues relating to the processing of personal data
- Informing, advising and issuing recommendations to the data controller and processor

Article 35(1) highlights that while it is the task of the data controller to carry out data protection privacy impact assessments, the DPO can play a very important and useful role in assisting the controller. Advice should be sought from the DPO in terms of:

- Whether to carry out a PIA;
- What methodology to follow;
- Whether to carry out the PIA in-house or externally;
- What safeguards to put in place to mitigate against risks identified by the PIA (including organisational or technical measures); and
- Whether or not the PIA has been carried out in a way that is compliant with the GDPR

Person Specification:

In line with Article 37, the DPO must be selected on the basis of the following:-

- Expertise* in national and European data protection laws and practices (*depending on the sensitivity, complexity and amount of data an organization processes);
- integrity and high professional ethics;
- a commensurate level of and an in depth understanding of the GDPR;
- an understanding of both the processing operations carried out and information technologies and data security of the organisation;
- knowledge of the business sector and the organisation; and
- the ability to promote a data protection culture within the organization.

J.4

Margaret Keyse

From: Crerar J (Janice) <Janice.Crerar@parliament.scot>
Sent: 29 March 2017 16:52
To: Rosemary Agnew
Cc: Hughes K (Ken); Margaret Keyse; David Lowrie
Subject: RE: 2017 03 29 - follow up to meeting

Dear Rosemary

Many thanks. I intend to set up a meeting in late May/early June with the officeholders' staff to discuss the DPO job role and specification (based on the Article 29 data Protection Working Party guidance) and the likely size of the DPO role in each of the offices to get a handle on whether we could provide a DPO shared service (assuming that is what officeholders want) or if we should procure the service and have the officeholders named on the contract.

Kind regards

Janice

The Scottish Parliament
Pàrlamaid na h-Alba

Mrs Janice Crerar
Officeholder Services
The Scottish Parliament
Edinburgh
EH99 1SP

Telephone: 0131 348 6851
email – janice.crerar@parliament.scot

From: Rosemary Agnew [mailto:ragnew@itspublicknowledge.info]
Sent: Wednesday, March 29, 2017 2:58 PM
To: Crerar J (Janice)
Cc: Hughes K (Ken); Margaret Keyse; David Lowrie
ubject: 2017 03 29 - follow up to meeting

Janice

When we met recently we briefly discussed two issues in addition to the budget:

1. Data Protection Officer

[redacted]

Hope these comments are helpful. Sorry it took so long, but I wanted to go back and review the DPO position.

Get back to me or Margaret with any questions.

Rosemary

Data Protection Officer

1. I explained my understanding from a presentation given to us about GDPR by Anderson Strathern (slides attached) was that the DPO could not be a shared service because of independence and conflicts of interest. This was relayed verbally during the presentation.

2. On reviewing the slides before I sent them to you, I realise that the text does not cover this, so we have revisited this. Having looked afresh at the legislation and the associated Article 29 Guidelines, our view is that a shared service is possible, but with certain and specific provisions.

3. There is nothing specifically in the guidelines which suggest that, for data controllers such as us, we can't share a DPO with another data controller. The focus in the guidelines (as well as in the GDPR) is on making sure, taking account of organisational structure and size, that a single DPO can perform their tasks efficiently, despite being responsible for several public authorities. This means they must be accessible and able to respond to each of the bodies they cover, at the times needed, either physically, via a hotline or other secure means of communication.

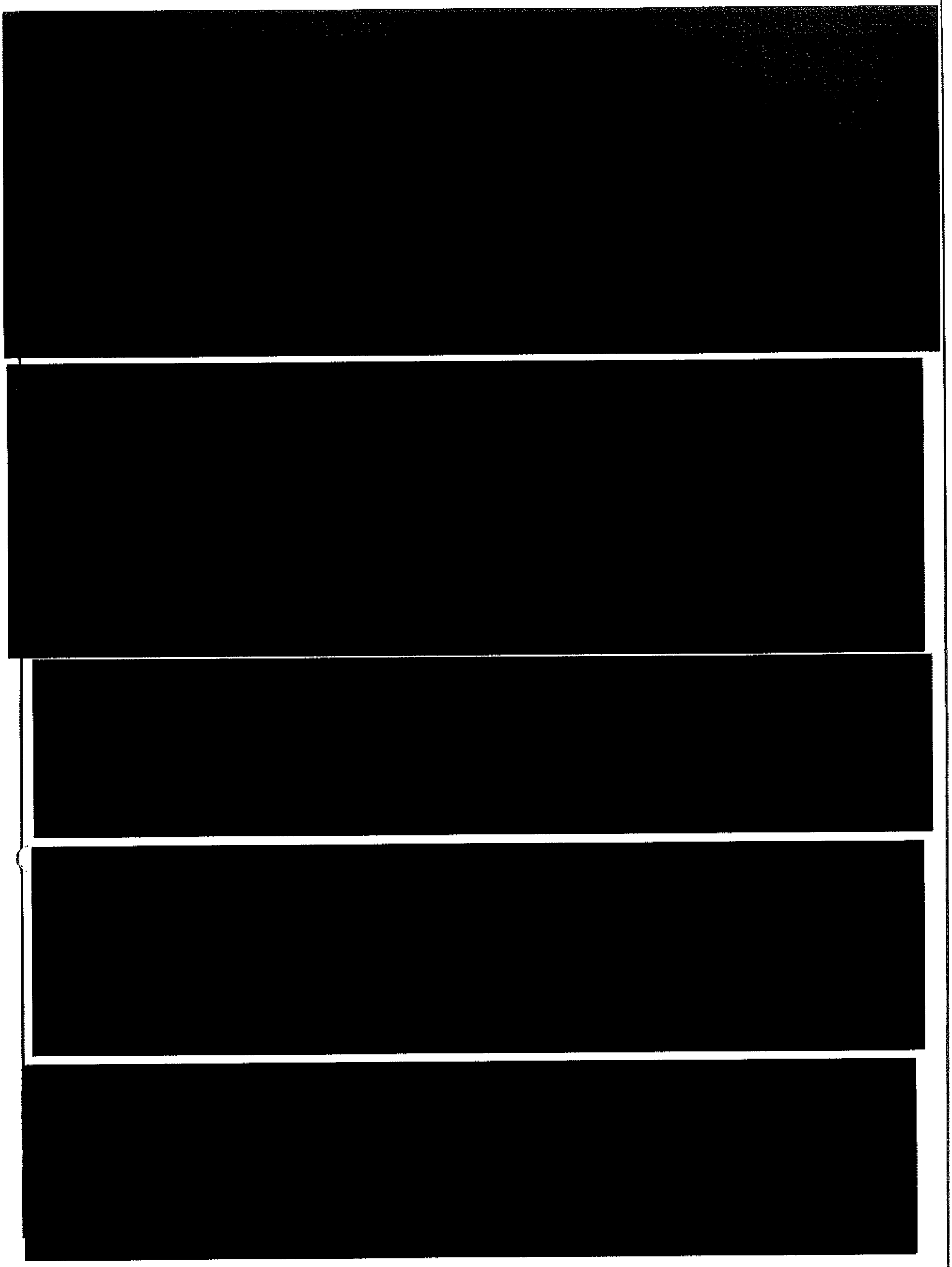
4. DPOs will be bound by secrecy or confidentiality concerning their performance of their tasks, in accordance with EU or Member State law (Article 38(5)). The DPO would be providing a service to several office holders, all of whom have a different legislative framework that could confer different duties and restrictions on them. For example, for us, despite their "independence", the DPO will remain subject to section 45 of FOISA for all work done on behalf of the Commissioner and disclosure will be a criminal offence unless done with lawful authority.

5. Given the wording of the GDPR and the guidelines, a shared service is, therefore, possible but I can understand that there might be some disquiet about us sharing a DPO with the bodies we regulate (and, at least in the case of the SPSO, with bodies which regulate us). While, the focus of the DPO is on data governance as a whole, rather than on decisions to be taken by the Commissioner in response to applications made under FOISA or the EIRs, I can envisage this might be where a conflict, or perceived conflict, of interest would come in.

6. I see no reason why, particularly in the light of section 45 of FOISA, we couldn't draw up an agreement which designed to avoid conflict of interests while allowing the DPO to carry out their full tasks under the GDPR.

7. The option of a shared procurement for a "DPO service" is still there if that is something the office holders would prefer.

[redacted]



[redacted]

Rosemary Agnew
Scottish Information Commissioner

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: ragnew@itspublicknowledge.info
Web: www.itspublicknowledge.info

Scottish Information Commissioner
it's public knowledge

www.itspublicknowledge.info or email: enquiries@itspublicknowledge.info

Scottish Information Commissioner, Kinburn Castle, Doubledykes Road,
St Andrews, Fife, KY16 9DS
Tel: 01334 464610 Fax: 01334 464611

S. S

Helen Gardner-Swift

From: Rosemary Agnew
Sent: 12 April 2017 09:53
To: 'Crerar J (Janice) (Janice.Crerar@parliament.scot)'
Cc: Helen Gardner-Swift; Jann Wallace
Subject: 2017 04 12 Data Protection Officer

Janice

Thanks for your email to Jann (who is off at the moment).

Helen Gardner-Swift, my new Head of Corporate Services and Jann will attend the meeting at 2.30 on 8 June.

We have a few questions we thought it might be helpful to raise in advance rather than spring them on you on the day:

1. Is the proposal to appoint an employee of the Parliament, whose job is to provide the shared DPO service to the office holders, or is the proposal to outsource to a third-party provider?

2. Assuming it is an employee, will this be someone new, or an existing member of staff?

3. Who will line manage the person? Our view is they should be line managed in your team, as it is a service to the office holders. This would reduce any potential for conflict of interest for those of us who "Regulate".

4. Will the person's role be exclusively DPO or will they have other Parliamentary duties? If not exclusive, how do you envisage the person managing and balancing competing demands on time, and on keeping reporting and functions separate?

5. Will each office holder have their own service level agreement/ contract, that sets out accessibility arrangements, confidentiality arrangements and escalation arrangements if there are any issues?

Rosemary

Rosemary Agnew
Scottish Information Commissioner

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: ragnew@itspublicknowledge.info
Web: www.itspublicknowledge.info

Scottish Information Commissioner
it's public knowledge

S. 6

Helen Gardner-Swift

[redacted]

From: Crerar J (Janice) [mailto:Janice.Crerar@parliament.scot]
Sent: 14 August 2017 15:43
To: Clare C. Nicolson <Clare.Nicolson@scottishhumanrights.com>; Helen (Helen.Littlemore@spso.gsi.gov.uk) <Helen.Littlemore@spso.gsi.gov.uk>; Helen Gardner-Swift <hgardnerswift@itspublicknowledge.info>; Karen Elder <k.elder@ethicalstandards.org.uk>; McLean El (Elaine) <E.McLean@standardscommission.org.uk>; Munro Gillian (Gillian.Munro@cypcs.org.uk) <Gillian.Munro@cypcs.org.uk>; Stephen Grounds <Stephen.Grounds@cypcs.org.uk>; Valerie.Malloch@spso.gsi.gov.uk
Subject: GDPR

Dear All

We have been looking at what we are required to do in respect of the new GDPR regulations covering data protection that take effect from 25 May 2018. Over the last few days you may have noticed this is gaining more media coverage. I am grateful to you all for your attendance at meetings we have held to date on this matter.

In going forward we (the SPCB) are taking a two-phased approach. Phase 1 is to ensure we are compliant in terms of the new regulatory framework. We would be keen to undertake this as a shared project with all officeholders. In practice, what this will mean from our side is a commitment to share the documentation we use, to make spaces available at training/ workshops for staff, as appropriate, to provide advice and generally to share best practice. Another advantage we would see from undertaking this as a shared approach would be for a uniformity in how all offices implement the regulations. We would see the monthly meetings that are taking place as a good forum for discussing progress by each office and a valuable forum for all parties to share knowledge/best practice.

Phase 2 for the SPCB will be around the late Autumn when we look at the requirement for a DPO as part of the GDPR regime. We feel it is important that we take stock in the first instance in respect of compliance to have a better idea of what this post will actually do. Again, we would be happy to share our thinking on this and also whether or not we could offer this as a shared service.

I hope that you would all be content to work together with us on Phase 1 which will not only save money but at the same time build up expertise in each office by way of a collaborative approach. I would be grateful if you could let me know if this is acceptable.

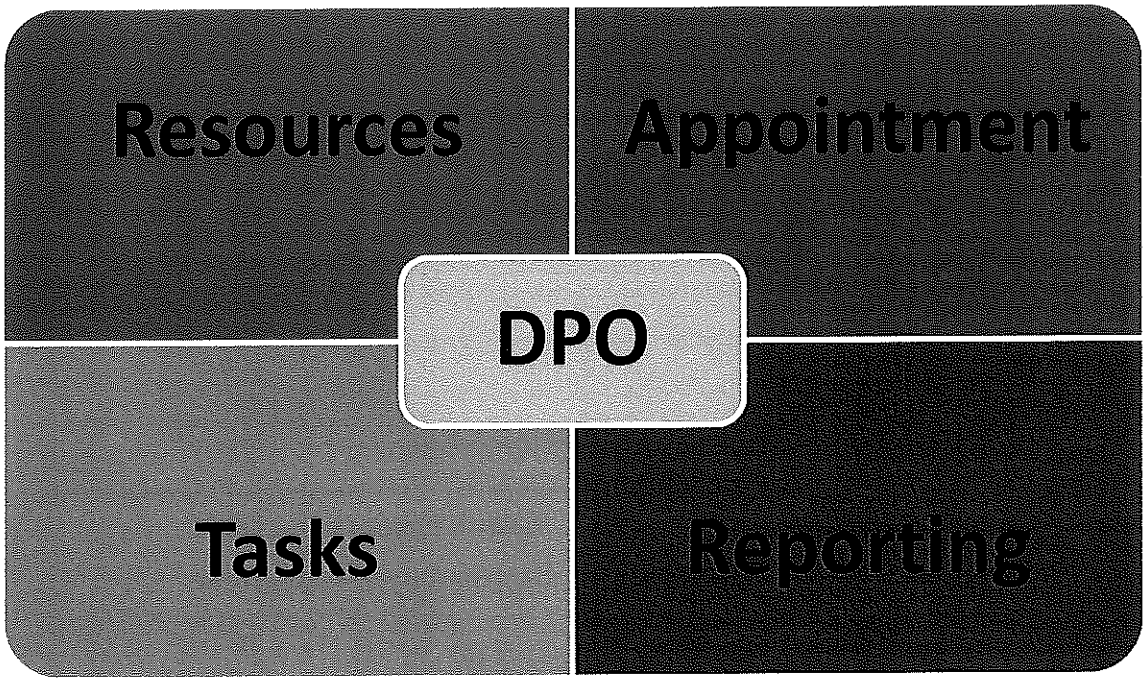
Kind regards

Janice

Mrs Janice Crerar
Officeholder Services
The Scottish Parliament
Edinburgh
EH99 1SP
Telephone: 0131 348 6851
email – janice.crerar@parliament.scot

6.)

DRAFT – notes – decision making – DPO
To be amended for each organisation to take into account the relevant decision making/governance criteria



DRAFT – notes – decision making – DPO
To be amended for each organisation to take into account the relevant decision making/governance criteria

Resources

Requirements

(1) In-house costs re: changing/implementing new procedures, etc

(2) Additional IT requirements

(3) Employment/contract costs of DPO - will vary depending on whether employee or contractor

(4) DPO resources

- must be sufficiently well resourced
- access to staff and other services - HR, IT, legal, security
- in-house or included in service contract?

Funding

(1) Absorb into existing budget

(2) No provision in budget - contingency funding?

(3) No provision in budget - contingency funding?

(4)No provision in budget - contingency funding?

N.B. Joint process for obtaining contigency funding?

DRAFT – notes – decision making – DPO
To be amended for each organisation to take into account the relevant decision making/governance criteria

Appointment

Requirements

to be appointed asap when preparing for GDPR

sufficient authority

sufficient autonomy

sufficient resources

easily accessible and contactable

to participate regularly in meetings with management

to be promptly consulted about any data breach

to have relevant professional qualities and expertise - commensurate with sensitivity, complexity and amount of data organisation processes

to manage any COI

Contract of Employment

Consider:

position in organisation

protection against dismissal

recruitment process

appointment process

fixed term contract

hours

terms and conditions

pay

Service Contract

SLA

accessibility arrangements

confidentiality

escalation provisions

contact arrangements

how many organisations sharing service?

data controller must ensure that a shared DPO can perform tasks efficiently despite being designated as DPO for several public authorities or bodies

costs - annual

fixed term

procurement process?

DRAFT – notes – decision making – DPO
To be amended for each organisation to take into account the relevant decision making/governance criteria

Tasks

Requirements (Art.39)

(1) Operate independently

(2) Sufficient degree of authority and direct reporting to senior management - how often?

(3) First point of contact for supervisory authorities and for individuals whose data is processed

(4) Monitor compliance with GDPR and other data protection laws

(5) PIA's

(6) Risk based and proportionate

(7) DPO training

Ensure

(1) Contract arrangements reflect the above - if an employee their professional duties must be compatible with the duties of a DPO and not lead to a COI and must not be responible for any data processing decisions

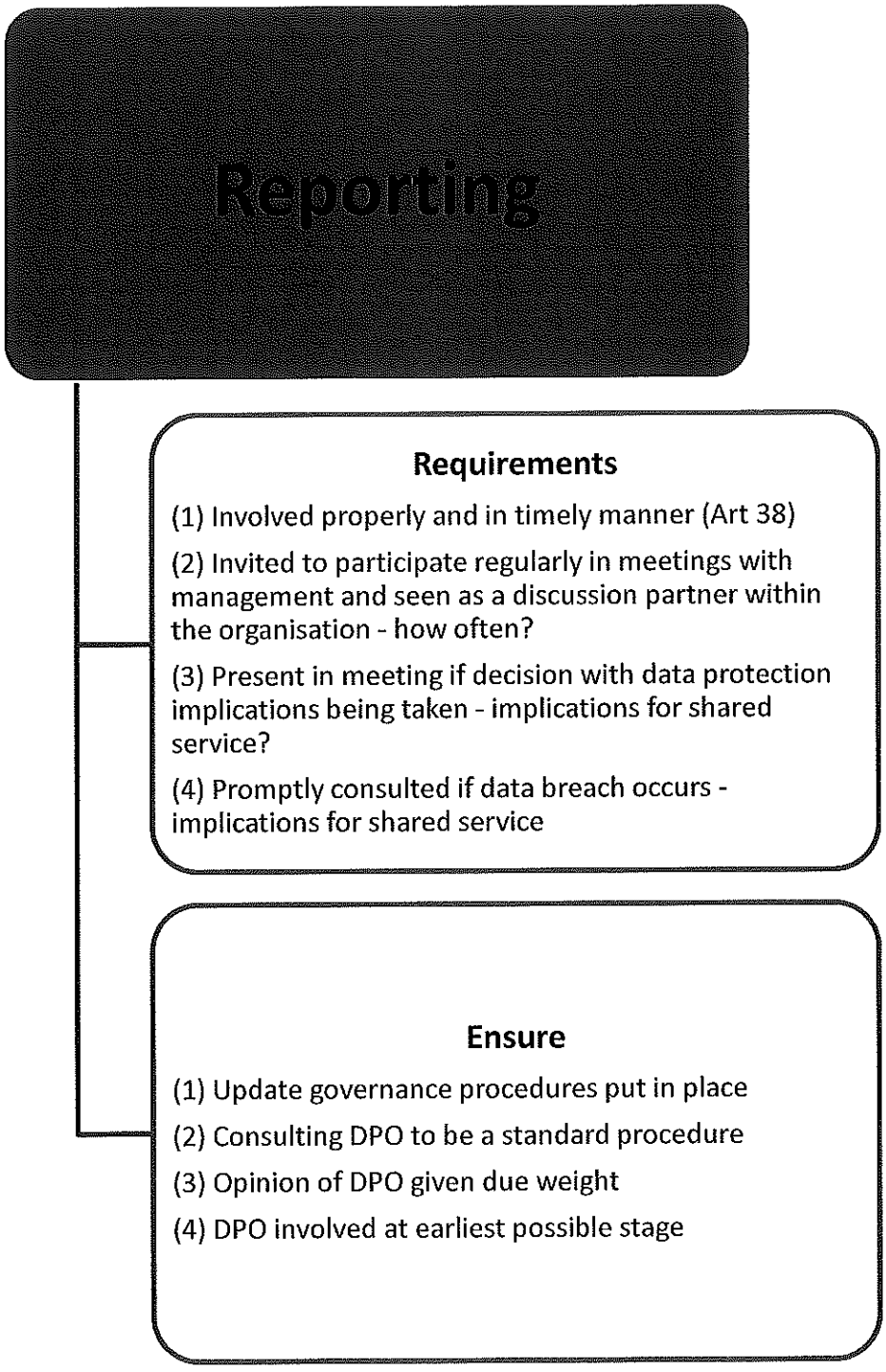
(2) Revised Governance arrangements and reporting requriements put in place

(3) Publication of contact arrangements

(4) Confidentiality for an individual contacting the DPO about their data

(5) Active support of DPO's function by senior management

DRAFT – notes – decision making – DPO
To be amended for each organisation to take into account the relevant decision making/governance criteria



Information Governance/Data Protection Specialists

Computer Law Training

http://computerlaw.org.uk/consultancy/#VDPO

This is a small company based in Central Scotland, specialising in data protection and information security. It was established in 2010 by Tim Musson. Tim is Convener of the Law Society of Scotland's Privacy Law Committee. Offering a virtual data protection officer service (meetings can be held online using conference software) with an initial data protection audit, annual audit and update and priority response to data protection issues. A quote for the service would be based on an initial meeting which would include a mini audit and assessment of needs. Previous clients include small law firms, Scottish local authorities and other public bodies.

Information Governance Training & Consultancy

http://www.infogov.scot/

Based in Central Scotland, and established in 2013 by Frank Rankin. Frank is a former Information Governance practitioner with 20 years' experience in central and local government and the NHS. I spoke to Frank to find out if this was a service he was intending to offer, and whether he was aware of other Scottish based firms that were offering this service. He was aware of a couple of legal firms that had mentioned provision of this type of service, but could not recall which ones. He had been thinking about offering such a service but currently very busy providing GDPR training, and therefore had not had the time to map out what this service would look like. He was keen to consider it a bit more and is going to provide us with a basic outline of what the outsourced service could look like which I will circulate when it arrives; he is hopeful that he will be able to send this week beginning 11 September. He discussed the need to provide a service in partnership with other Information Governance specialists.

Law Firms

Anderson Strathern

I had a very helpful conversation with Fiona Killen (Partner and Head of Parliamentary and Public Law Unit) about an outsourced service. This is something Fiona has thought about however with a team of two it would be difficult to offer this service. Fiona felt that to provide a good level of service they would need detailed knowledge of an organisation's IT system, and quite a lot of direct involvement with the organisation. Fiona went through a list of other considerations:

1. Using a law firm for this service would be a costly way to do it as we would be paying legal firm costs. She thought it would be as cost effective to employ someone on a part-time basis to do this. She also suggested it would be wiser to set aside a budget for specific legal advice to assist in responding to the very difficult data protection issues.

2. As far as Fiona is aware other organisations (e.g. local authorities etc. are holding off on recruiting a DPO at least until December/January. Basically, they are waiting until later in the day to a) save costs and b) ensure the appointed DPO can audit GDPR processes and procedures independently from the organisation.

3. Fiona recommends putting in place as much of the GDPR requirements as possible before designating a DPO, therefore focus on the preparation and training of the organisation.

4. She does think a shared service approach across all the Officeholders is possibly our best option. We also discussed the extent to which the DPO could be resourced internally. Is there a staff member who could undertake the necessary training to skill up on data protection? Need to write into employment contracts that the DPO can act in an independent matter to ensure necessary safeguards are in place for them.

Macroberts
I've arranged to discuss an outsourced service with David Gourlay (Compliance and Regulatory Team).

Other Companies
Sapphire Consulting
https://sapphireconsulting.co.uk/
Based in Cornwall. Offer a full range of consultancy services, including an outsourced DPO service. As a minimum, they only require one contracted hour per month for their DPO service. Also offer a DPO recruitment service. No indication of costs. Company incorporated in October 2016, and looks like it really is a sole trader. Testimonials are very limited.

Aphaia
https://aphaia.co.uk/en/
Based in London. A small company incorporated in 2009 that offers a Data Protection Officer outsourcing service. This service is offered from £375 per month plus VAT. This includes ongoing support including a limited number of phone calls and written documents and a bespoke report every month plus. Additional hours are priced at £100 per month. Case studies are primarily provision of privacy advice to small tech start-ups.

BSI
https://www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/Services/Data-Protection-GDPR/
Offering an outsourced Data Protection Officer service. No indication of costs or how the service would operate.

6.3

Helen Gardner-Swift

From: Karen Elder <k.elder@ethicalstandards.org.uk>
Sent: 21 August 2017 15:11
To: Helen Gardner-Swift
Cc: Clare.Nicolson@scottishhumanrights.com; Helen.Littlemore@spso.gsi.gov.uk; E.McLean@standardscommission.org.uk; Gillian.Munro@cypcs.org.uk; Stephen.Grounds@cypcs.org.uk; Valerie.Malloch@spso.gsi.gov.uk; sharon.barbour@scottishhumanrights.com; emculloch@itspublicknowledge.info; Bill Thomson; Crerar J (Janice) (Janice.Crerar@parliament.scot)
Subject: FW: DPO - draft specification

Dear Helen

Thank you for the preparing this draft DPO specification - it's very helpful and great starting point. We agree with the general principle of having a single contract giving an overview of the services required with sub-contracts or schedules describing the work required for each office-holder. This will assist the supplier in quoting and us in apportioning costs to each office-holder.

We have three general issues to raise:

1. General. We would like to clarify further what tasks will be done by the DPO and what by the office-holder's inhouse DP team. Given that DPA services are an additional cost, the inhouse team should carry out as much as possible.
2. Section 2.3. We consider that an initial contract for three years with extension for 2 years would be appropriate. Given how new the DPO role is and that they will be required to build up detailed knowledge of office-holders work a shorter contract might not be effective. We recognise that a three year contract would require robust assessment procedures to ensure that any issues with the contract are managed and resolved promptly.
3. Section 5. We consider it more appropriate to appoint one provider and invite them to explain as part of the tender how conflicts of interest will be managed. Multiple contractors are likely to add costs as they would need to build up knowledge of each client's processes.

On the specifics

- Section 2.1. Meetings, advice, consultation and contact - final bullet. *The DPO will be expected to be able to be promptly contacted and consulted once a data breach or incident has occurred.* We would also welcome their assistance in identifying **whether** a data breach has occurred.
- Section 2.1. Monitoring compliance - final bullet. *Monitoring duties may include acting as the contact point for the supervisory authority on issues relating to the processing of personal data.* We recognise that this is listed in Art39 but are concerned about how this will work in practice. How do we mitigate the risk of the DPO not fully understanding how we process personal data and mis-conveying that to the ICO? There will be data audits and flow-charts, etc but the DPO will need to hold and understand that information for six or seven organisations.

Helen you asked some specific questions. These are either noted or agreed, except in relation to our view on HG8 (see item 2 above) and we would welcome discussion on HG11 – 17.

If you need any clarification please let me know.

Kind regards, Karen

Karen Elder
Business Manager
Commissioner for Ethical Standards in Public Life in Scotland
Thistle House
91 Haymarket Terrace

Edinburgh
EH12 5HE
Tel: 0131 347 3898
www.ethicalstandards.org.uk

From: Helen Gardner-Swift [mailto:hgardnerswift@itspublicknowledge.info]
Sent: 31 July 2017 09:26
To: Clare.Nicolson@scottishhumanrights.com; Helen.Littlemore@spso.gsi.gov.uk; Karen Elder <k.elder@ethicalstandards.org.uk>; E.McLean@standardscommission.org.uk; Gillian.Munro@cypcs.org.uk; Stephen.Grounds@cypcs.org.uk; Valerie.Malloch@spso.gsi.gov.uk; sharon.barbour@scottishhumanrights.com; emculloch@itspublicknowledge.info; Bill Thomson <b.thomson@ethicalstandards.org.uk>
Cc: Crerar J (Janice) <Janice.Crerar@parliament.scot>
Subject: DPO - draft specification

Dear All,

I refer to the last meeting of the GDPR working group on 27 June 2017 and have attached the draft specification/heads of terms for a DPO service agreement. I am sorry that I have not been able to circulate this earlier (I needed to spend more time with our auditors on the annual report than I originally estimated).

The draft specification is very much a working draft and will need more details included. My comments indicate the matters that I have identified that need to be considered further at this time and there may be other relevant issues that will need to be referred to in the document. I hope the attached provides a useful base from which to discuss this matter further and go forward. Please could you forward this email to anyone that I have missed from my circulation list.

I look forward to seeing you tomorrow at 1130.

Kind regards,

Helen

Helen Gardner-Swift

Head of Corporate Services

Scottish Information Commissioner

Kinburn Castle, Doubledykes Road

St Andrews, KY16 9DS

Tel: 01334 464625

Fax: 01334 464611

Email: hgardnerswift@itspublicknowledge.info

Web: www.itspublicknowledge.info

Twitter: @FOIScotland

DRAFT SPECIFICATION OF REQUIREMENTS

FOR THE PROVISION OF A DATA PROTECTION OFFICER TO THE OFFICE HOLDERS

1. Introduction

The SPCB [and Office Holders] need to retain a Data Protection Officer ("DPO") for each Office Holder and wish to appoint a firm/company ('the Service Provider') to provide data protection officer services as described at paragraph 3 below to the Office Holders.

Comment [HG1]: Need to determine who will be the client/contracting party. If solely the SPCB will there then need to be MOU's between SPCB and Office Holders relating to the provision of DPO services?

Comment [HG2]: Need to consider the appropriate description.

2. Background: Scope, Value and Contract Duration

2.1 Scope

Each Office Holder is required to retain a Data Protection Officer ("DPO") and this contract will cover the data protection officer service required by each of the Office Holders.

A DPO's primary concern is to enable compliance with the GDPR and it is crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection for each Office Holder.

General requirements

Meetings, advice, consultation and contact

For each Office Holder, the DPO will be expected:-

- to participate regularly in meetings of senior management (and where also required middle management);
- to participate in meetings where decisions with data protection implications are taken.
- to provide opinions and advice on matters relating to data protection.
- to be able to be promptly contacted and consulted once a data breach or incident has occurred.

Monitoring compliance

The DPO has a duty to monitor compliance with the GDPR. Monitoring duties may include:

Comment [HG3]: ART. 39(1)(b) and Recital 97

- collecting information to identify processing activities
- awareness-raising, and training of staff involved in the processing operations, and the related audits
- providing advice where required as regards the data protection impact assessment and monitoring its performance in line with Article 35
- co-operating with the supervisory authority (ICO in the UK)
- analysing and checking compliance of processing activities
- acting as the contact point for the supervisory authority on issues relating to the processing of personal data
- informing, advising and issuing recommendations to the data controller and processor

Privacy Impact Assessments

As data controller, an Office Holder, may need to carry out data protection privacy impact assessments and, if so, the DPO will be expected to advise the Office Holder on the following :

- whether to carry out a PIA;
- what methodology to follow;
- whether to carry out the PIA in-house or externally;
- what safeguards to put in place to mitigate against risks identified by the PIA (including organisational or technical measures); and
- whether or not the PIA has been carried out in a way that is compliant with the GDPR

Accessibility

The DPO must be accessible to and available to communicate with and respond to each Officer Holder whenever necessary (as each Office Holder is a data processor and/or controller and has data subjects).

Autonomy

The DPO must perform their tasks with a sufficient degree of autonomy and each Office Holder will ensure that the DPO does not receive any instructions regarding the exercise of his or her tasks.

For each Officer Holder, the DPO will report directly to the highest management level.

Confidentiality

The DPO will be bound by confidentiality in the performance of their tasks.

Each Office Holder has a different statutory framework that confers different duties and restrictions.[*details to be provided*]

2.2 Value

The value of the contract as described here with reference to fees plus VAT is approximately £..... per annum.

2.3 Contract Duration

The contract will commence in [.....2017] (exact date to be confirmed) and will run for one/two/three years until [.....20..], with an option to extend the contract for 2 further 12-month periods subject to satisfactory performance.

3. The Service

3.1 DPO specification

Each of the Office Holders is required to have a DPO who must meet the following requirements:

- Expertise* in national and European data protection laws and practices (*depending on the sensitivity, complexity and amount of data an organisation processes);
- integrity and high professional ethics;

Comment [HG4]: Art 35(1)(a).

Comment [HG5]: Need to provide the relevant details for each Office Holder. For example, for SIC, the DPO will also be subject to section 45 of FOISA for all work done on behalf of the SIC and disclosure will be a criminal offence unless done with lawful authority

Comment [HG6]: Will need to determine this.

Comment [HG7]: This value of the contract will also help to determine the relevant procurement route.

Comment [HG8]: Office Holder views needed on this.

Comment [HG9]: Who will assess this?

- a commensurate level of and an in depth understanding of the GDPR;
- an understanding of both the processing operations carried out and information technologies and data security of the organisation;
- knowledge of the business sector and the organisation; and
- the ability to promote a data protection culture within the organization.

3.2 Service to be provided to each Office Holder

Each Office Holder will require the following:

Comment [HG10]: The matters set out at 2.1 above are general and there will need to be included in this section the specific requirements for each Office Holder , for example, number of meetings that DPO will be expected to attend, the amount of time, etc that the DPO will need to be available to them, the accessibility arrangements, etc.

4. Delivery of Services

A draft Service Level Agreement (SLA) must be produced by each tenderer for consideration, demonstrating how they intend to undertake the DPO role for each Office Holder.

The structure of the SLA will need to allow flexibility in the levels of service to be delivered to each Office Holder and some form of a multi–level SLA - upper level/corporate SLA applying to all and then individual Service Level Management Arrangement ("SLMA") applying to each office holder – will need to be put in place to cover the following:

SLA content

- introduction
- generic issues – same for each organisation to be covered
- service description – what service the SLA supports and details of the service
- mutual responsibilities
- conflict of interests
- confidentiality
- security
- costs and charging method

Comment [HG11]: Are there any particular requirements concerning this?

SLMA content

- applicable service for each office holder
- contact points & escalation – communication framework

This draft SLA will form part of the evaluation exercise.

5. CONFLICT OF INTEREST SERVICE PROVIDERS

The Service Provider will provide data protection services to each of the Office Holders and will be able undertake other tasks and duties, as regards each of the Officer Holders, as long as they do not constitute a conflict of interest.

Comment [HG12]: Need more detail on what might constitute a "conflict of interest" and need to consider this further. For example, Given the wording of the GDPR and the guidelines, a shared service is, possible there might be some disquiet about SIC sharing a DPO with the bodies that SIC regulates (and, at least in the case of the SPSO, with bodies which regulate SIC). While, the focus of the DPO is on data governance as a whole, rather than on decisions to be taken by the SIC in response to applications made under FOISA or the EIRs, it is possible that this might be where a conflict, or perceived conflict, of interest would arise.

It is our intention to award the contract to [3] Service Providers. [The 2nd and 3rd ranked Service Providers shall be used only in the event of a conflict of interest between [the .....and .....]

Comment [HG13]: Will this be required?

6. Contract Management and Administration

Comment [HG14]: Who will instruct the Service Provider

[*Details of the Contract Manager and instruction processes will need to be included here*].

Comment [HG15]: Who will manage the contract – the SPCB

The Service Provider will be expected to put in place named relationship management contacts and escalation arrangements.

The Service Provider will be expected to submit monthly financial and allocation management information to the contract manager which will include (but will not be limited to):

[*list of matters that will need to provide information on*]

There will be a quarterly review with the Service Provider and the Service Provider will meet to discuss the Service Level requirements and general performance. The frequency of these reviews can be changed as and when it is felt necessary and appropriate.

Comment [HG16]: Need to decide on the frequency of any review.

Comment [HG17]: Need to decide how the review will be carried out and who will do this.

No charge of any kind shall be made by the Service Provider in respect of compliance with these performance reviews.

7. Fees and Invoicing

The rates offered by the appointed Service Provider will apply for the term of two years from commencement of the contract and for any contract extension period.

[*fee invoicing and estimates arrangements need to be included*]

Helen Gardner-Swift

From: Gillian Munro <Gillian.Munro@cypcs.org.uk>
Sent: 28 August 2017 16:52
To: Helen Gardner-Swift
Subject: RE: GDPR - DPO minute of 3rd meeting 2017.08.01 draft

Dear Helen,

My apologies for missing the comments deadline of the 25 August. I am just back from holiday and ran out of time to email you before I left. As Steve has overall responsibility for managing contracts on behalf of the Commissioner's office he is best placed to provide feedback on the duration of the contract [HG8] and whether a 2nd and 3rd ranked service provider will be required [HG13]. As indicated by Karen, I think further discussion of the other comments you have raised at the next monthly meeting may be the best way to progress these.

I only have one addition to make under 2.1 Accessibility regarding the need for the DPO to also be accessible and available to communicate with and respond to data subjects, with a corresponding requirement under 3.1 DPO specification that they have the ability to communicate clearly with data subjects.

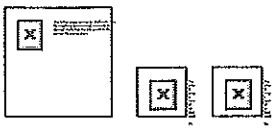
Hope that all makes sense, and thank you for all the work you have undertaken in preparing the draft DPO specification.

Kind regards
Gillian

Gillian Munro
Children & Young People's Commissioner Scotland
Rosebery House
Ground Floor
9 Haymarket Terrace
Edinburgh
EH12 5EZ

Tel: 0131 346 5350
Fax: 0131 337 1275
Young Persons' Freephone: 0800 019 1179

www.cypcs.org.uk



DPO – draft specification – comments from members of SPCB GDPR Working Party (up and until 7 September 2017)

DPO Specification Issued 31/07/17	HG comment on draft specification	Response/Comments from members of SPCB GDPR Working Party
1	Need to determine who will be the client/contracting party. If solely the SPCB will there then need to be MOU's between SPCB and Office Holders relating to the provision of DPO services?	**Ethical Standards – noted/agreed**
2	Need to consider the appropriate description e.g, firm, company	**Ethical Standards – noted/agreed**
3		
4		
5	Need to provide the relevant details for each Office Holder. For example, for SIC, the DPO will also be subject to section 45 of FOISA for all work done on behalf of the SIC and disclosure will be a criminal offence unless done with lawful authority	**Ethical Standards – noted/agreed**
6	Will need to determine the value p.a.	**Ethical Standards – noted/agreed**
7	This value of the contract will also help to determine the relevant procurement route	**Ethical Standards – noted/agreed**
8	Office Holder views needed on contract duration.	**Ethical Standards – consider that an initial contract for three years with extension for 2 years would be appropriate. Given how new the DPO role is and that they will be required to build up detailed knowledge of office-holders work a shorter contract might not be effective. We recognise that a three year contract would require robust assessment procedures to ensure that any issues with the contract are managed and**

		resolved promptly. **CYCSP – SG to comment**
9	Who will assess performance of service provider?	**Ethical Standards – noted/agreed**
10	The matters set out at 2.1 are general and there will need to be included in this section the specific requirements for each Office Holder , for example, number of meetings that DPO will be expected to attend, the amount of time, etc that the DPO will need to be available to them, the accessibility arrangements, etc.	**Ethical Standards – noted/agreed**
11	Are there any particular requirements concerning security?	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**
12	Need more detail on what might constitute a "conflict of interest" and need to consider this further. For example, Given the wording of the GDPR and the guidelines, a shared service is, possible there might be some disquiet about SIC sharing a DPO with the bodies that SIC regulates (and, at least in the case of the SPSO, with bodies which regulate SIC). While, the focus of the DPO is on data governance as a whole, rather than on decisions to be taken by the SIC in response to applications made under FOISA or the EIRs, it is possible that this might be where a	**Ethical Standards – welcome discussion - consider it more appropriate to appoint one provider and invite them to explain as part of the tender how conflicts of interest will be managed. Multiple contractors are likely to add costs as they would need to build up knowledge of each client's processes.** **CYCSP – welcome discussion**

	conflict, or perceived conflict, of interest would arise.	
13	How many service providers will be required?	**Ethical Standards – welcome discussion** **CYCSP – SG to comment**
14	Who will instruct the Service Provider?	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**
15	Who will manage the contract – the SPCB?	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**
16	Need to decide on the frequency of any review with the Service Provider?	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**
17	Need to decide how the review will be carried out and who will do this.	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**
	Other Comments from members of SPCB GDPR Working Party	
	General	**Ethical Standards** - **agree with the general principle of having a single contract giving an overview of the services required with sub-contracts or schedules describing the work required for each office-holder - this will assist the supplier in quoting and us in apportioning costs to each office-holder.** - **would like to clarify further what tasks will be done by the DPO and what by the office-holder's inhouse DP team. Given that DPA services are an additional cost, the inhouse team should carry out as much as possible.**
2.1	**Meetings, advice, consultation and contact**	• **final bullet.** ***The DPO will be expected to be able to be promptly contacted and***

	For each Office Holder, the DPO will be expected:- • to participate regularly in meetings of senior management (and where also required middle management); • to participate in meetings where decisions with data protection implications are taken. • to provide opinions and advice on matters relating to data protection. • to be able to be promptly contacted and consulted once a data breach or incident has occurred.	***consulted once a data breach or incident has occurred.*** **We would also welcome their assistance in identifying whether a data breach has occurred.** **CYCSP - accessibility regarding the need for the DPO to also be accessible and available to communicate with and respond to data subjects, with a corresponding requirement under , 3.1 DPO specification that they have the ability to communicate clearly with data subjects.**
2.1	**Monitoring compliance** The DPO has a duty to monitor compliance with the GDPR. Monitoring duties may include: • collecting information to identify processing activities • awareness-raising, and training of staff involved in the processing operations, and the related audits • providing advice where required as regards the data protection impact assessment and monitoring its performance in line with Article 35 • co-operating with the supervisory authority (ICO in the UK) • analysing and checking compliance of processing activities • acting as the contact point for the supervisory authority on issues relating to the processing of personal data	**Ethical Standards - Monitoring duties may include acting as the contact point for the supervisory authority on issues relating to the processing of personal data. We recognise that this is listed in Art39 but are concerned about how this will work in practice. How do we mitigate the risk of the DPO not fully understanding how we process personal data and mis-conveying that to the ICO? There will be data audits and flow-charts, etc but the DPO will need to hold and understand that information for six or seven organisations.**

	• informing, advising and issuing recommendations to the data controller and processor	

VC 92481

DPO – draft specification – comments from members of SPCB GDPR Working Party/Office Holders (up and until 10 September 2017)

DPO Specification Issued 31/07/17	HG comment on draft specification	Response/Comments from members of SPCB GDPR Working Party
1	**Introduction** Need to determine who will be the client/contracting party. Need to consider the appropriate description. If solely the SPCB will there then need to be MOU's between SPCB and Office Holders relating to the provision of DPO services?	Ethical Standards – noted/agreed Ethical Standards – noted/agreed
2	**Background: Scope, Value and Contract Duration**	
2.1	**Meetings, advice, consultation and contact** For each Office Holder, the DPO will be expected:- • to participate regularly in meetings of senior management (and where also required middle management); • to participate in meetings where decisions with data protection implications are taken. • to provide opinions and advice on matters relating to data protection. • to be able to be promptly contacted and consulted once a data breach or incident has occurred.	Ethical standards • **final bullet. *The DPO will be expected to be able to be promptly contacted and consulted once a data breach or incident has occurred.* We would also welcome their assistance in identifying whether a data breach has occurred.** **CYCSP - accessibility regarding the need for the DPO to also be accessible and available to communicate with and respond to data subjects, with a corresponding requirement under , 3.1 DPO specification that they have the ability to communicate clearly with data subjects.** **SPSO - additional bullets:** • **to inform and advise the Office Holders and their employees about their obligations to comply with the GDPR and other data protection laws;** • **SPSO - to be present**

96

		• **to help implement essential elements of the GDPR.** RA - regular meetings & participate in meetings - it should be made clear that this is in an advisory capacity to ensure we were taking the correct things into account and in the right way. I think the work participate is wrong and should be "attend in advisory capacity" Also they may not be regular so the word is not needed, and they are by invitation. RA – promptly contacted - this needs setting out into a proper timescale: ie immediate, same working day etc. Also where is cover to come from if the DPO is away?
2.1	**Monitoring compliance** The DPO has a duty to monitor compliance with the GDPR. (ART. 39(1)(b) and Recital 97) Monitoring duties may include: • collecting information to identify processing activities • awareness-raising, and training of staff involved in the processing operations, and the related audits • providing advice where required as regards the data protection impact assessment and monitoring its performance in line with Article 35 • co-operating with the supervisory authority (ICO in the UK) • analysing and checking compliance of processing activities • acting as the contact point for the supervisory authority on issues relating to the processing of personal data	**Ethical Standards - monitoring duties may include acting as the contact point for the supervisory authority on issues relating to the processing of personal data. We recognise that this is listed in Art39 but are concerned about how this will work in practice. How do we mitigate the risk of the DPO not fully understanding how we process personal data and mis-conveying that to the ICO? There will be data audits and flow-charts, etc but the DPO will need to hold and understand that information for six or seven organisations.** **SPSO - additional bullets:** • **advise on data protection impact assessments,** • **conduct internal audits,** • **be the first point of contact for supervisory authorities (ICO) and for individuals whose data is processed (employees, customers etc),** • **handle complaints? (see UKG statement of intent 7/8/17)**

	• informing, advising and issuing recommendations to the data controller and processor	
2.1	**PIA** - Art 35(1)(a).	
2.1	**Accessibility**	**SPSO - DPO to be easily accessible both externally and internally.** RA - see earlier comment about definitive timescales for agreement
2.1	**Autonomy**	**SPSO - Operate independently and not led by the organisation.**
2.1	**Confidentiality** Need to provide the relevant details for each Office Holder. For example, for SIC, the DPO will also be subject to section 45 of FOISA for all work done on behalf of the SIC and disclosure will be a criminal offence unless done with lawful authority	**SPSO - Section 19 of the Scottish Public Services Ombudsman Act 2002**
2.2	**Contract value** Will need to determine this. The value of the contract will also help to determine the relevant procurement route.	**Ethical Standards – noted/agreed**

2.3	**Contract duration** Need office holders' views on this. Who will assess performance?	**Ethical Standards – consider that an initial contract for three years with extension for 2 years would be appropriate. Given how new the DPO role is and that they will be required to build up detailed knowledge of office-holders work a shorter contract might not be effective. We recognise that a three year contract would require robust assessment procedures to ensure that any issues with the contract are managed and resolved promptly.** **CYCSP – SG to comment** **SPSO - would we want to start out with a one year contract?**
3.1	**DPO Specification**	**Expertise – SPSO - DPO should have professional experience and knowledge of data protection law and practice (and other relevant laws such as common law of confidentiality and human rights).**
3.1	**Service to be provided to each office holder** The matters set out at 2.1 above are general and there will need to be included in this section the specific requirements for each Office Holder , for example, number of meetings that DPO will be expected to attend, the amount of time, etc that the DPO will need to be available to them, the accessibility arrangements, etc.	**Ethical Standards – noted/agreed** **SPSO** • **Eight formal SMT meetings a year, in addition to informal ad-hoc meetings that the DPO may be expected to attend.** • **24/7 availability for ad-hoc consultation, advice, incident handling, complaints etc.** • **Accessible 24/7 by phone or video link (currently around 90 plus employees and advisers, and over 6k contacts from customers per year).**

		• Visits to be arranged in advance.
4	**Delivery of services** **SLA content**	**SPSO** • Service standards • Quality measures • Security – demonstrate appropriate security measures in place • Retention and disposal • Contact/visiting arrangements • Review • Termination – notice period of 3 months, in writing? RA - what about conflict resolution and complaints if we have an issue? Who do we go to?
4	**Delivery of services** **SLA content** Are there any particular requirements concerning security?	Ethical Standards – welcome discussion CYCSP – welcome discussion
5	**Conflict of Interest**	

	Need more detail on what might constitute a "conflict of interest" and need to consider this further. For example, Given the wording of the GDPR and the guidelines, a shared service is, possible there might be some disquiet about SIC sharing a DPO with the bodies that SIC regulates (and, at least in the case of the SPSO, with bodies which regulate SIC). While, the focus of the DPO is on data governance as a whole, rather than on decisions to be taken by the SIC in response to applications made under FOISA or the EIRs, it is possible that this might be where a conflict, or perceived conflict, of interest would arise. No. of contract services providers? - Will this be required and, if so, how many?	**Ethical Standards – welcome discussion - consider it more appropriate to appoint one provider and invite them to explain as part of the tender how conflicts of interest will be managed. Multiple contractors are likely to add costs as they would need to build up knowledge of each client's processes.** **CYCSP – welcome discussion** **SPSO - my understanding for this is that the DPO can't have a role in determining how and what personal data is used (they will just provide advice).** **Ethical Standards – welcome discussion** **CYCSP – SG to comment**
6	**Contract Management and Administration** Who will instruct the Service Provider? Who will manage the contract – the SPCB? Need to decide on the frequency of any contract review. Need to decide how the contract review will be carried out and who will do this.	**Ethical Standards – welcome discussion** **CYCSP – welcome discussion**

7	**Value of contract** This value of the contract will also help to determine the relevant procurement route	Ethical Standards – noted/agreed
	General	Ethical Standards – we would like to clarify further what tasks will be done by the DPO and what by the office-holder's inhouse DP team. Given that DPA services are an additional cost, the inhouse team should carry out as much as possible.

DPO – draft specification – comments from members of SPCB GDPR Working Party/Office Holders (up and until 11 October 2017)

(1) • thank you for responding
• this is intended as a working doc to aid discussion thinking

DPO Specification Issued 31/07/17	HG comment on draft specification	Response/Comments from members of SPCB GDPR Working Party
1	**Introduction** Need to determine who will be the client/contracting party. Need to consider the appropriate description. If solely the SPCB will there then need to be MOU's between SPCB and Office Holders relating to the provision of DPO services?	**Ethical Standards – noted/agreed** **Ethical Standards – noted/agreed** **(New) CYPCS – Preference is for SPCB to be the contracting party and sub contract to office holders through either MOU or SLA**
2	**Background: Scope, Value and Contract Duration**	
2.1	**Meetings, advice, consultation and contact** For each Office Holder, the DPO will be expected:- • to participate regularly in meetings of senior management (and where also required middle management); • to participate in meetings where decisions with data protection implications are taken. • to provide opinions and advice on matters relating to data protection. • to be able to be promptly contacted and consulted once a data breach or incident has occurred.	Ethical standards • **final bullet. *The DPO will be expected to be able to be promptly contacted and consulted once a data breach or incident has occurred.* We would also welcome their assistance in identifying whether a data breach has occurred.** **(New) CYPCS – Clarification on "middle management" – we don't have a "middle management" group so this wouldn't be required in CYPCS** **CYPCS - accessibility regarding the need for the DPO to also be accessible and available to communicate with and respond to data subjects, with a corresponding requirement under , 3.1 DPO specification that they have the ability to communicate clearly with data subjects.** **SPSO - additional bullets:**

(2) • Preference for SPCB to be the contracting party with MOU or SLA – others may have views

• cover provisions important if only 1 DPO.

(3) • different types of [illegible] structure could need to be catered for
• access requirement to be provided for whether advisory not [illegible]

6.7

		• **to inform and advise the Office Holders and their employees about their obligations to comply with the GDPR and other data protection laws;** • **SPSO - to be present** • **to help implement essential elements of the GDPR.** RA - regular meetings & participate in meetings - it should be made clear that this is in an advisory capacity to ensure we were taking the correct things into account and in the right way. I think the work participate is wrong and should be "attend in advisory capacity" Also they may not be regular so the word is not needed, and they are by invitation. RA – promptly contacted - this needs setting out into a proper timescale: ie immediate, same working day etc. Also where is cover to come from if the DPO is away? **(New) CYPCS – The question of "cover" should be included in the specification and included in the contract. Would we require some sort of "exclusivity" so that the DPO works exclusively to the SPCB and Office Holders?**
2.1	**Monitoring compliance** The DPO has a duty to monitor compliance with the GDPR. (ART. 39(1)(b) and Recital 97) Monitoring duties may include: • collecting information to identify processing activities • awareness-raising, and training of staff involved in the processing operations, and the related audits • providing advice where required as regards the data protection impact assessment and monitoring its performance in line with Article 35	**Ethical Standards - monitoring duties may include acting as the contact point for the supervisory authority on issues relating to the processing of personal data. We recognise that this is listed in Art39 but are concerned about how this will work in practice. How do we mitigate the risk of the DPO not fully understanding how we process personal data and mis-conveying that to the ICO? There will be data audits and flow-charts, etc but the DPO will need to hold and understand that information for six or seven organisations.** **(New) CYPCS – It might be possible to address Ethical Standards point about risk of DPO not fully understanding how we process personal data via a 'Record of Processing Activities' (see Article 30), although may be that not all Officeholders will be required to maintain such a record.**

• work out what will be the Complaint process in place (from next round)

(4). How will DPO fully understand at diff ways that office holders process info & diff. purposes

• Mention of "Record of Processing Activities" ⇒ compare

2

	• co-operating with the supervisory authority (ICO in the UK) • analysing and checking compliance of processing activities • acting as the contact point for the supervisory authority on issues relating to the processing of personal data • informing, advising and issuing recommendations to the data controller and processor	**SPSO - additional bullets:** • **advise on data protection impact assessments,** • **conduct internal audits,** • **be the first point of contact for supervisory authorities (ICO) and for individuals whose data is processed (employees, customers etc),** • **handle complaints? (see UKG statement of intent 7/8/17)**
2.1	**PIA** - Art 35(1)(a).	
2.1 (5)	**Accessibility** • DPO need easily accessible & will need to be cover arrangement in place.	**SPSO - DPO to be easily accessible both externally and internally.** **(New) CYPCS – See previous comment on arrangements for "cover". Any arrangements for cover need to take account of DPO being accessible to Officeholders, employees and data subjects.** **RA - see earlier comment about definitive timescales for agreement**
2.1 (6)	**Autonomy** Agreement – DPO will operate independently & be subject to instruction by office holders. or SPCB	**SPSO - Operate independently and not led by the organisation.** **(New) CYPCS – Operate independently and not led by SPCB or Office Holders**
2.1	**Confidentiality** Need to provide the relevant details for each Office Holder. For example, for SIC, the DPO will also be subject to section 45 of FOISA for all work done on	**SPSO - Section 19 of the Scottish Public Services Ombudsman Act 2002** **(New) CYPCS – We don't have any specific duty or restriction in our Act regarding confidentiality. However, is included in our own separate standard terms and**

(7) • Diff reqt ~~statutory~~ requirements, (including staff requirements for cover), for each office holder will need to be taken into a/c → in the contract built into a MOU/SLA

	behalf of the SIC and disclosure will be a criminal offence unless done with lawful authority	**conditions when contracting with suppliers**
2.2	**Contract value** Will need to determine this. The value of the contract will also help to determine the relevant procurement route.	**Ethical Standards – noted/agreed** **(New) CYPCS – Think this should read "The value and length" of the contract. If over 3 years then the overall value will help to determine the procurement route.** • suggestion that length of contract also determines procurement route.
2.3	**Contract duration** Need office holders' views on this. Who will assess performance? (7) • Range of views • 3 yrs – 1 yr • perhaps 2 yrs satisfy all? • officeholders also need to provide feedback re performance to SPCB could collate into & make overall assessment of perform	**Ethical Standards – consider that an initial contract for three years with extension for 2 years would be appropriate. Given how new the DPO role is and that they will be required to build up detailed knowledge of office-holders work a shorter contract might not be effective. We recognise that a three year contract would require robust assessment procedures to ensure that any issues with the contract are managed and resolved promptly.** **(New) CYPCS – Consider that the initial contract should be for three years with an optional extension for an annual rolling contract.** **(New) CYSP – All Officeholders provide feedback/assessment of performance as part of MOU with SPCB. SPCB then in position to collate this information and make an overall assessment of performance of DPO service provider.** **SPSO - would we want to start out with a one year contract?**
3.1	**DPO Specification**	**Expertise – SPSO - DPO should have professional experience and knowledge of data protection law and practice (and other relevant laws such as common law of**

(8) ~~DO~~ DPO needs to be experienced & appropriately qualified

		confidentiality and human rights).
3.1	**Service to be provided to each office holder** The matters set out at 2.1 above are general and there will need to be included in this section the specific requirements for each Office Holder , for example, number of meetings that DPO will be expected to attend, the amount of time, etc that the DPO will need to be available to them, the accessibility arrangements, etc. (9) Again range of requirement in regard to service SPSO - 8 formal meeting CYPCS - 6 " " SIC - 4 " " will need to be available 24/7 ? (72 hrs reporting requirement re: breaches) ICO.	**Ethical Standards – noted/agreed** **SPSO** • **Eight formal SMT meetings a year, in addition to informal ad-hoc meetings that the DPO may be expected to attend.** • **24/7 availability for ad-hoc consultation, advice, incident handling, complaints etc.** • **Accessible 24/7 by phone or video link (currently around 90 plus employees and advisers, and over 6k contacts from customers per year).** • **Visits to be arranged in advance.** **(New) CYPCS – Estimate six formal meetings in first year with a review at year end. Then possibly meetings held quarterly in years two and three.**
4	**Delivery of services** **SLA content** (10) SLA MOU would need to deal with - service standard, - quality measures - security of info - retention + disposal of info - contact - review - complaint process + contact resolution } Each officeholder will need to set out their part. requirement.	**SPSO** • **Service standards** • **Quality measures** • **Security – demonstrate appropriate security measures in place** • **Retention and disposal**

		• **Contact/visiting arrangements** • **Review** • **Termination – notice period of 3 months, in writing?** RA - what about conflict resolution and complaints if we have an issue? Who do we go to? **(New) CYPCS – Conflict resolution and complaints – possible 3 options:** • **Would the Office Holder contact SPCB in the first instance?** **or** • **Would the Office Holder contact the DPO direct keeping SPCB informed and then come back to SPCB if not resolved?**
4	**Delivery of services** **SLA content** Are there any particular requirements concerning security?	**Ethical Standards – welcome discussion** **(New) CYPCS – Would require DPO to have PVG Scheme clearance as would have access to children and young people's personal data and they may (as data subjects) contact DPO direct. Clearance would also be required for staff/individuals providing DPO cover arrangements.**
5	**Conflict of Interest** Need more detail on what might constitute a "conflict of interest" and need to consider this further. For example, Given the wording of the GDPR and the guidelines, a shared service is, possible there might be some disquiet about SIC sharing a DPO with the bodies that SIC regulates (and, at least in the case of the SPSO, with bodies which regulate SIC). While, the focus of the DPO is	**Ethical Standards – welcome discussion - consider it more appropriate to appoint one provider and invite them to explain as part of the tender how conflicts of interest will be managed. Multiple contractors are likely to add costs as they would need to build up knowledge of each client's processes.** **CYPCS – welcome discussion**

(11) Addl. requirement may be needed for delivery of service eg CYPCS ⇒ PVG reqd

-direct contact / PVG

(12) Report started

→ respondent all welcome discussion on this

→ SPSO of view that DPO doesn't have a role in determining how & what personal data used? → simply providing advice

	on data governance as a whole, rather than on decisions to be taken by the SIC in response to applications made under FOISA or the EIRs, it is possible that this might be where a conflict, or perceived conflict, of interest would arise. No. of contract services providers? - Will this be required and, if so, how many?	**SPSO - my understanding for this is that the DPO can't have a role in determining how and what personal data is used (they will just provide advice).** **Ethical Standards – welcome discussion** **(New) CYPCS – Happy to discuss as not sure this is required**
6	**Contract Management and Administration** Who will instruct the Service Provider? Who will manage the contract – the SPCB? Need to decide on the frequency of any contract review. Need to decide how the contract review will be carried out and who will do this. (13) All respondent welcome discussion	**Ethical Standards – welcome discussion** **CYPCS – welcome discussion**
7 (14)	**Value of contract** This value of the contract will also help to determine the relevant procurement route	**Ethical Standards – noted/agreed**
(15)	**General** → repeat this	**Ethical Standards – we would like to clarify further what tasks will be done by the DPO and what by the office-holder's inhouse DP team. Given that DPA services are an additional cost, the inhouse team should carry out as much as possible.**

- now talk about way forward
- will SPCB be taking this on? –

DPO – draft specification – comments from members of SPCB GDPR Working Party/Office Holders (up and until 11 October 2017)

GDPR Working Party – DPO Specification (to be discussed 12/101/7) – HGS points

- Thank everyone who provided comments for doing this
- Draft specification should be viewed as a working document – assist with the consideration of this service provision and how/whether it should be put in place
- Helpful to run through the various sections of the draft specification and highlight the comments raised
- Then decide next steps – this is in Phase 2 of work on GDPR but need to keep in mind???

1. Introduction

Contracting party – expressed preference for the SPCB to be the contracting party and sub contract to office holders through MOU or SLA

2. Background: Scope, Value and Contract Duration

2.1 Meetings, advice, consultation and contact

- DPO need to be promptly contacted and consulted re: data breaches and be accessible to data subjects
- Also need assistance from DPO to establish whether data breach occurred
- Not all office holders have a middle management group
- Difference of opinion on whether the DPO needs to regularly attend meetings and whether they will be expected to participate or simply attend in an advisory capacity
- Consider the requirements re: cover to be provided by DPO and exclusivity

Monitoring compliance

- DPO will need to understand personal data for several organisations concern about how monitoring duties will work in practice – DPO may not fully understand how officeholder processes personal data and misconvey information to DPO - possible solution to have "Record of Processing Activities" (N.B. data audit leads you to putting such a record in place)
- Will the DPO also handle complaints? (see UKG statement of intent 7/8/17 – SPSO comment)

Accessibility

- DPO needs to be accessible both internally and externally – see also previous comments re: cover and timescales

Autonomy

- Office holders act/operate independently and not led by SPCB or other office holders

Confidentiality

- Different requirements re: confidentiality – need to be taken into account in MOU or SLA

2.2 Contract value

- Refer instead to value and length of contract - help to determine the procurement route

2.3 Contract duration

- Contract duration – vies range from 3 year to 1 year – go for 2 years?

3. DPO Specification

- DPO will need to have professional experience and knowledge of dp law and other relevant laws e.g common law (confidentiality) and human rights

3.1 Service to be provided to each office holder

- Range of requirement for DPO to attend meetings
  - SPSO – 8 formal meetings
  - CYPCS – 6 formal meetings
  - SIC – 4 formal meetings

4. Delivery of Services – SLA content

- Range of matters to be included (and will need to be thought about in more detail by each office holder if go forward with the shared service) – service standards, quality measures, security, retention and disposal of records, contact/visiting arrangements, review, termination, conflict resolution and complaints
- Re: complaints would office holder contact SPCB in first instance or the DPO and keep SPCB in loop
- Particular requirements – CYCPS – require DPO to have PVG scheme clearance

5. Conflict of Interest

- Discussion on this would be welcomed – do this now?
- See SIC views on comment sheet

6. Contract Management and Administration

- Discussion on this welcomed – do this now?
- See SIC views on comment sheet

7. Value of Contract

- Noted that the value of the contract will help to determine the relevant procurement route

General

- There needs to be clarification on what tasks will be carried out by the DPO and what by the Office Holder's in-house team
- In-house team carry out as much as possible?

7.1

Margaret Keyse

From: Lorraine Currie
Sent: 21 March 2018 17:26
To: Margaret Keyse; Daren Fitzhenry; Helen Gardner-Swift; Euan McCulloch
Subject: RE: 20180321-MOU for DPO services

In Virtual Cabinet: 0

I've added my comments and changes too.

With regard to clause 7, last year I drafted an escalation clause to be included in the hosting and support contract with C2 (our website provider). This was based on based on the Scottish Government Service Level Agreement, and the text is in VC 91198 (see page 4).

Thanks
Lorraine

Lorraine Currie
Freedom of Information Officer

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: lcurrie@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

From: Margaret Keyse
Sent: 21 March 2018 16:39
To: Daren Fitzhenry; Helen Gardner-Swift; Lorraine Currie; Euan McCulloch
Subject: RE: 20180321-MOU for DPO services

I've suggested quite a few changes – although they're really tidy-ups rather than changes to the MoU.

I've suggested adding quite a bit about the law enforcement provisions in the DPA 2018. However, given that we're the only "competent authority" (for law enforcement purposes) that will have to comply with that bit, it may be that we just suggest that if others are going to use this as a template then they ignore those references.

Margaret

From: Daren Fitzhenry
Sent: 21 March 2018 14:59
To: Helen Gardner-Swift; Lorraine Currie; Euan McCulloch; Margaret Keyse
Subject: 20180321-MOU for DPO services
Importance: High

Dear All,

I have now made some suggested amendments to the MOU for DPO services with the SPCB. Following on from earlier inputs and discussions, I have put an emphasis on full DPO service, confidentiality, agency (s 45 of FOISA), and conflicts of interest, all of which are necessary if we are able to use the shared service. I have put the amended MOU into VC 100183. Can I please ask you, as members of the GDPR working group, to give this an urgent review, with any further additions/amendments to be made by 1200 tomorrow (Thur 22 Mar), so that Helen can then send it off to the SPCB for their consideration?

Apologies for the short fuse on this one, but many thanks for your help.

Kind Regards

Daren

Daren Fitzhenry
Scottish Information Commissioner

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: dfitzhenry@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter @FOIScotland

Margaret Keyse

From: Euan McCulloch
Sent: 21 February 2018 14:47
To: Helen Gardner-Swift
Cc: Daren Fitzhenry; Margaret Keyse; Lorraine Currie
Subject: FW: GDPR - DPO
Attachments: GDPR - DPO 9th Meeting - Agenda 20180215.docx; Draft MEMORANDUM OF UNDERSTANDING DPO Services 20171030.docx

In Virtual Cabinet: 0

Given that Claire is a primary point of contact for our investigations (when the Parliament/SPCB is the public authority), the scope for conflict would be fairly marked

Euan McCulloch
Deputy Head of Enforcement

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: emcculloch@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

From: Helen Gardner-Swift
Sent: 21 February 2018 13:50
To: Daren Fitzhenry
Cc: Margaret Keyse; Euan McCulloch; Lorraine Currie
Subject: FW: GDPR - DPO

Daren,

I have been in contact with the SPSO again (Helen Littlemore). Helen L has been advised Claire Turnbull, Head of Information Governance, Information Governance & Management Team, Scottish Parliament will be the DPO under the proposed MOU (assisted by a team). Helen L is seeking further comments from the Ombudsman before tomorrow's meeting, however, is also of the view that the potential conflicts of management and the perception by members of the public (who may have to contact the DPO) that the DPO may lack the required independence may be difficult to overcome.

If you have any further thoughts please can you let me know before by the end of today, if possible.

Helen

From: Euan McCulloch
Sent: 16 February 2018 15:35
To: Helen Gardner-Swift
Cc: Margaret Keyse; Lorraine Currie; Daren Fitzhenry
Subject: FW: GDPR - DPO

Helen

I would suggest that the first line of clause 2 should refer to "the services of a named Data Protection Officer (DPO), as follows:" – at present, it appears to be purporting to offer a less specific DPO service, with only some of the subsequent bullets referring to the services of a named DPO.

That said, there must be significant concerns if the same officer could also be doing DP work for the SPCB – particularly if no thought has been given to conflicts of interest.

Euan McCulloch
Deputy Head of Enforcement

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: emcculloch@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

From: Helen Gardner-Swift
Sent: 15 February 2018 16:27
To: Margaret Keyse; Euan McCulloch; Lorraine Currie
Cc: Daren Fitzhenry
Subject: FW: GDPR - DPO

Hello,

I will place this on the agenda for next week's Working Party meeting, however, it would be helpful if you let me have your initial views.

I have asked Janice to confirm who will be the intended DPO and which team within the SPCB he/she will be located in.

I will be looking at the DPO's responsibilities, as set out in the proposed MOU, as I researched this when this subject was discussed at earlier SPCB GDPR meetings and will also look at the terms of the MOU – I note that the provisions relating to Conflict of Interests and Dispute Resolution are blank – as this ties in with the work that I did on the draft specification.

Helen

From: Crerar J (Janice) [mailto:Janice.Crerar@parliament.scot]
Sent: 15 February 2018 16:14
To: Claire Gilmore (c.gilmore@ethicalstandards.org.uk); Clare C. Nicolson; Euan McCulloch; Helen

Margaret Keyse

From: Lorraine Currie
Sent: 21 February 2018 17:30
To: Helen Gardner-Swift
Subject: RE: GDPR - DPO

In Virtual Cabinet: 0

Hi Helen,

Just to confirm, I've no comments beyond what Euan's already raised.

Thanks
Lorraine

Lorraine Currie
Freedom of Information Officer

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: lcurrie@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

From: Helen Gardner-Swift
Sent: 21 February 2018 13:50
To: Daren Fitzhenry
Cc: Margaret Keyse; Euan McCulloch; Lorraine Currie
Subject: FW: GDPR - DPO

Daren,

I have been in contact with the SPSO again (Helen Littlemore). Helen L has been advised Claire Turnbull, Head of Information Governance, Information Governance & Management Team, Scottish Parliament will be the DPO under the proposed MOU (assisted by a team). Helen L is seeking further comments from the Ombudsman before tomorrow's meeting, however, is also of the view that the potential conflicts of management and the perception by members of the public (who may have to contact the DPO) that the DPO may lack the required independence may be difficult to overcome.

If you have any further thoughts please can you let me know before by the end of today, if possible.

Helen

From: Euan McCulloch
Sent: 16 February 2018 15:35
To: Helen Gardner-Swift
Cc: Margaret Keyse; Lorraine Currie; Daren Fitzhenry
Subject: FW: GDPR - DPO

Helen

I would suggest that the first line of clause 2 should refer to "the services of a named Data Protection Officer (DPO), as follows:" – at present, it appears to be purporting to offer a less specific DPO service, with only some of the subsequent bullets referring to the services of a named DPO.

That said, there must be significant concerns if the same officer could also be doing DP work for the SPCB – particularly if no thought has been given to conflicts of interest.

Euan McCulloch
Deputy Head of Enforcement

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464610
Fax: 01334 464611
Email: emcculloch@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

From: Helen Gardner-Swift
Sent: 15 February 2018 16:27
To: Margaret Keyse; Euan McCulloch; Lorraine Currie
Cc: Daren Fitzhenry
Subject: FW: GDPR - DPO

Hello,

I will place this on the agenda for next week's Working Party meeting, however, it would be helpful if you let me have your initial views.

I have asked Janice to confirm who will be the intended DPO and which team within the SPCB he/she will be located in.

I will be looking at the DPO's responsibilities, as set out in the proposed MOU, as I researched this when this subject was discussed at earlier SPCB GDPR meetings and will also look at the terms of the MOU – I note that the provisions relating to Conflict of Interests and Dispute Resolution are blank – as this ties in with the work that I did on the draft specification.

Helen

From: Crerar J (Janice) [mailto:Janice.Crerar@parliament.scot]
Sent: 15 February 2018 16:14
To: Claire Gilmore (c.gilmore@ethicalstandards.org.uk); Clare C. Nicolson; Euan McCulloch; Helen

(Helen.Littlemore@spso.gsi.gov.uk); Helen Gardner-Swift; Karen K. Elder; McLean El (Elaine); Mcleod IIG (Isla); Munro Gillian (Gillian.Munro@cypcs.org.uk); Sharon S. Barbour; Stephen Grounds; Turnbull CM (Claire); Valerie.Malloch@spso.gsi.gov.uk
Subject: GDPR - DPO

Dear All

Please find attached an agenda for next week's meeting.

As you are aware, the SPCB is keen to share services wherever possible to make financial savings. The offer of access to the SPCB's DPO and his/her team would be at nil cost.

I attach a draft MOU for discussion (really is a starter for 10.....) and it would be helpful to get an indication at the meeting if this offer is something that you will wish to avail yourself of.

I have drafted it as an MOU but happy to discuss if this is the best way forward.

Kind regards

Janice

Mrs Janice Crerar
Officeholder Services
The Scottish Parliament
Edinburgh
EH99 1SP
Telephone: 0131 348 6851
email – janice.crerar@parliament.scot

Memorandum of Understanding

Between

[Commissioner/Ombudsman/Commission**]**

And

The Scottish Parliamentary Corporate Body

This Memorandum of Understanding is drawn up to provide a basis on which the **officeholder** (henceforward known as the Commissioner/Ombudsman/Commission) and the Scottish Parliamentary Corporate Body (henceforward known as the SPCB) may develop a relationship, specifically for the provision of data protection officer services under the General Data Protection Regulations that will come into force on 25 May 2018.

1. Background

The General Data Protection Regulations will provide a modernised, accountability-based compliance framework for data protection. Data protection officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the GDPR. The GDPR lays down conditions for the appointment, position and tasks of the DPO.

Under the GDPR, it is mandatory for public authorities to designate a DPO. Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment.

Under the Shared Services Agenda for officeholders, the SPCB will make available to the [Commissioner/Ombudsman/Commission], at nil cost, a DPO service.

Details of the service to be provided are set out below.

2. General

The SPCB will provide Data Protection Officer services as follows:-

- A named DPO to attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;
- A DPO to attend, by invitation, such other meetings/working groups dealing with data processing activities;
- To provide advice to the Commissioner/Ombudsman/Commission on matters relating to data protection;
- Provide advice to the Commissioner/Ombudsman/Commission where requested as regards the DPIA and monitor its performance including (i) whether or not to carry out a DPIA; (ii) what methodology to follow when carrying out a DPIA; (iii) whether to carry out the DPIA in-house or whether to outsource it; (iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; (v) whether or not the data protection impact assessment has been correctly carried out and (vi) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR;

- Inform and advise the [Commissioner/Ombudsman/Commission] and their employees about their obligations to comply with the GDPR and other data protection laws;
- Assist the [Commissioner/Ombudsman/Commission] to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance is set out in paragraph X below;
- Co-operate with the supervisory body (ICO)) and act as a contact point for the supervisory authority on issues relating to processing, prior consultation and to consult, where appropriate, with regard to any other matter;
- Act as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and
- A named DPO to be accessible and available to communicate [efficiently and clearly] with and respond to data subjects (breach notifications/the right to access/the right to be forgotten).

3. Compliance

The named DPO will not be personally responsible for non-compliance with the GDPR.

Data protection compliance is the responsibility of the controller or the processor.

The DPO will assist the [Commissioner/Ombudsman/Commission] to monitor compliance by:-

- Informing themselves fully of how the [Commissioner/Ombudsman/Commission] processes data ideally through a flowchart or equivalent;
- advising on data protection impact assessments;
- conducting internal audits;
- collecting information to identify processing activities;
- awareness-raising, through training of employees involved in the processing operations, and the related audits;
- providing advice where required as regards the data protection impact assessment and monitoring its performance in line with Article 35;
- co-operating with the supervisory authority (ICO);
- analysing and checking compliance of processing activities;
- informing, advising and issuing recommendations to the data controller and processor;
- acting as the contact point for the supervisory authority on issues relating to the processing of personal data;
- informing, advising and issuing recommendations to the data controller and processor; and
- Being available to employees and data subjects.

4. Accessibility

The named DPO and his/her team will be accessible to the [Commissioner/Ombudsman/Commission] as follows:-

Activity	Timescale
Attend senior management meetings where data protection issues are being discussed	As timetabled
Providing advice on data protection issues	On receipt of all relevant information:- Non urgent - within X working days

	Urgent – X working days
Training	
Assisting the [Commissioner/Ombudsman/Commission] to determine if there has been a breach	Within X working days
Assisting the [Commissioner/Ombudsman/Commission] where a data breach or incident has occurred	Be contactable by phone within X hours of the [Commissioner/Ombudsman/Commission] becoming aware that a breach has occurred

5. Confidentiality

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority (ICO).

6. Conflicts of interest

7. Dispute resolution

8. Role of Commissioner/Ombudsman/Commissions

The Commissioner/Ombudsman/Commissions will:-

- publish contact details of the DPO
- communicate the contact details of the DPO to the relevant supervisory authorities
- promptly consult with the DPO once a data breach or another incident has occurred
- maintain a record of processing operations under his/her/its responsibility;
- provide the DPO which sufficient information to enable the DPO to accurately rely information to the ICO on how they process personal data. This will ideally be in the form of a flowchart.
- provide the DPO with contact details for his/her office.
- liaise with the DPO to timetable routine meetings, training sessions and other meetings will be arranged as and when required giving the DPO at least 4 weeks advance notice.
- co-operate with the DPO and his/her team
- invite the DPO to be present where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

- give the opinion of the DPO due weight. If there is a disagreement, the reasons for not following the DPO's advice should be documented;

- ensure that if its data processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO will be given the opportunity to make his or her dissenting opinion clear to the Commissioner/Ombudsman/Commissions

- shall seek the DPO's advice when carrying out a DPIA;

- if they so choose, develop data protection guidelines or programmes that set out when the DPO must be consulted

7.2

Memorandum of Understanding

Between

[Commissioner/Ombudsman/Commission]

And

The Scottish Parliamentary Corporate Body

And

[The Data Protection Officer]

This Memorandum of Understanding is drawn up to provide a basis on which the **officeholder** (henceforward known as the Commissioner/Ombudsman/Commission) and the Scottish Parliamentary Corporate Body (henceforward known as the SPCB) may develop a relationship, specifically for the provision of data protection officer services under the General Data Protection Regulation (the GDPR) that comes into force on 25 May 2018 and the Data Protection Act 2018 [which comes into effect on ...].

1. Background

The General Data Protection Regulation and Data Protection Act 2018 provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the GDPR.

Under the GDPR, it is mandatory for public authorities to designate a DPO.

Under Part 3 of the DPA 2018, it is mandatory for "competent authorities", i.e. authorities which have statutory functions for the purposes of the prevention, investigation, detection or prosecution of criminal offences, etc. to designate a DPO for the purpose of those functions.

Both the GDPR and the DPA 2018 lay down conditions for the appointment, position and tasks of the DPO.

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment.

Similarly, Part 3 of the DPA 1998 allows the same person to be designated as a DPO by several controllers.

Under the Shared Services Agenda for officeholders, the SPCB will make available to the [Commissioner/Ombudsman/Commission], at nil cost, a DPO service.

Details of the service to be provided are set out below.

2. General

The SPCB will provide the Commissioner all DPO services, including law enforcement DPO services, as set out in the GDPR and DPA 2018. When carrying out DPO services

V05

Comment [HG1]: Yes –this should be included at this time

Comment [DF2]: Should there be a mechanism for the DPO to countersign the MOU as "named DPO" to show their awareness of the terms and functions/duties under the MOU?

Deleted: ¶

Comment [MK3]: Consider adding a reference to the Data Protection Act 2018 here?

May also be worth taking out reference to coming into force as this will age the MoU very quickly.

Deleted: Regulations

Deleted: will

Deleted: s will

Deleted: p

Moved down [1]: The GDPR lays down conditions for the appointment, position and tasks of the DPO.

Comment [MK4]: I've just referenced "Part 3" since we don't know what the final section numbers will be.

Comment [MK5]: We're the only competent authority which will be signing this MoU.

Moved (insertion) [1]

Deleted: The GDPR

Deleted: s

Comment [MK6]: Add text about DPA 2018 here? For example: "The DPA 2018

Deleted: ata Protection Officer

Deleted: Data Protection Act 2018

for the Commissioner, the DPO will be acting as the agent of the Commissioner. Without prejudice to the foregoing generality, the services provided to the Commissioner will include:-

- A named DPO to attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;
- A DPO to attend, by invitation, such other meetings/working groups dealing with data processing activities:
- To provide advice to the Commissioner/Ombudsman/Commission on matters relating to data protection;
- Provide advice to the Commissioner/Ombudsman/Commission where requested as regards the Data Protection Impact Assessment (DPIA) requirements in Section 3 of the GDPR and Chapter 4 of the DPA 2018 and monitor its performance including (i) whether or not to carry out a DPIA; (ii) what methodology to follow when carrying out a DPIA; (iii) whether to carry out the DPIA in-house or whether to outsource it; (iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; (v) whether or not the DPIA has been correctly carried out and (vi) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR and/or the DPA 2018;

- Inform and advise the [Commissioner/Ombudsman/Commission] and their employees about their obligations to comply with the GDPR, the DPA 2018 and other data protection laws;
- Assist the [Commissioner/Ombudsman/Commission] to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance is set out in paragraph X below.
- Co-operate with the supervisory authority (i.e. the Information Commissioner (ICO)) and act as a contact point for the supervisory authority on issues relating to processing, prior consultation and to consult, where appropriate, with regard to any other matter;
- Act as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and
- The named DPO to be accessible and available to communicate (efficiently and clearly) with and respond to data subjects (in relation to breach notifications/the right to access/the right to be forgotten).

3. Compliance

The named DPO will not be personally responsible for non-compliance with the GDPR and/or the DPA 2018.

Data protection compliance is the responsibility of the controller or the processor.

The DPO will assist the [Commissioner/Ombudsman/Commission] to monitor compliance by:-

- informing themselves fully of how the [Commissioner/Ombudsman/Commission] processes data ideally through a flowchart of equivalent;
- advising on DPIAs and Privacy Impact Assessments (PIAs);
- conducting internal audits;
- collecting information to identify processing activities;

Comment [DF7]: This is important as it brings the DPO under the section 45 of FOISA, which makes it an offence to disclose information obtained (unless the disclosure is made with lawful authority).

Deleted: follows

Deleted: data protection impact assessment

Deleted: body

Deleted: A

Deleted: [

Deleted:]

Formatted: Font: 11 pt

Deleted: I

Comment [MK8]: Is this a typo? A "flowchart of equivalent" might be a thing of course!

Comment [HG9]: Should we also include reference to PIAs?

Deleted: data protection impact assessments

- awareness-raising, through training of employees involved in the processing operations, and the related audits;
- providing advice where required as regards DPIAs and monitoring its performance in line with Article 35 of the GDPR/Chapter 4 of the DPA 2018;
- co-operating with the supervisory authority;
- analysing and checking compliance of processing activities;
- informing, advising and issuing recommendations to the data controller and processor;
- acting as the contact point for the supervisory authority on issues relating to the processing of personal data;
- informing, advising and issuing recommendations to the data controller and processor; and
- being available to employees and data subjects.

Deleted: the data protection impact assessment

Deleted: (ICO)

Deleted: B

4. Accessibility

The named DPO and his/her team will be accessible to the [Commissioner/Ombudsman/Commission] as follows:

Activity	Timescale
Attend senior management meetings where data protection issues are being discussed	As timetabled
Providing advice on data protection issues	On receipt of all relevant information:- Non urgent – within X working days Urgent – X working days
Training	
Assisting the [Commissioner/Ombudsman/Commission] to determine if there has been a breach	Within X working hours
Assisting the [Commissioner/Ombudsman/Commission] where a data breach or incident has occurred	Be contactable by phone within X hours of the [Commissioner/Ombudsman/Commission] becoming aware that a breach has occurred
Attend such other meetings/working groups dealing with data protection activities	

Comment [LC10]: Since the notification must be made within 72 hours of becoming aware of the breach, we shouldn't have to wait a number of working days after flagging a potential breach to the DPO for them to provide view on whether there has been a breach.

Deleted: days

Comment [LC11]: This is mentioned in clause 2 and we may want to call in the DPO to attend meetings of the GDPR working party, or meetings about project work which have an impact on our processing of personal data. Therefore, we should set some sort of "notice" to be given to the DPO, and timescale within which they will confirm attendance.

Comment [LC12]: There are other activities mentioned in clause 2 which should have timescales ascribed to them, e.g. acting as contact point with the ICO, or with data subjects about their rights.

5. Confidentiality

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks for the Commissioner. The Commissioner has specific duties under section 45 of the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (the EIRs) about maintaining confidentiality, and must ensure that his organisation maintains its independence and impartiality, and avoids conflicts of interest. Section 45 of FOISA and regulation 18 of the EIRs also apply to the DPO as agent of the Commissioner. In this context, all information received by the DPO from the Commissioner for the purposes of delivering services to the Commissioner shall be kept confidential and not be disclosed to any third party without the consent of the Commissioner, unless required to be disclosed by law or judicial decree. Third-party is understood to mean any person external to the office of the Scottish Information

Deleted: applies

Comment [MK13]: The disclosure will only be lawful under s45 if made in line with s45(2). Should we use the wording in s45(2)(c)(i) and (d) to reflect this? It would also be clear from that that it will not stop the DPO contacting etc the supervisory authority.

Commissioner. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.

6. Conflicts of interest

It is not anticipated that conflicts of interest are likely to arise. However, should any conflict of interest occur, or a situation arise in which it is considered that a conflict of interest is likely to occur, the DPO should immediately notify the Commissioner and will cease to provide DPO services to the Commissioner in relation to that conflict of interest. The Commissioner will, in such a situation, use alternative DPO services. The DPO will remain bound by the duties of secrecy and confidentiality, including their duties under section 45 of FOISA, in respect of any information obtained by them, as set out in paragraph 5 above.

7. Complaints and Dispute resolution

The Commissioner, the SPCB and the DPO shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the MOU within 20 working days of either party notifying the other in writing of the dispute.

The escalation process for any dispute will be:-

- As regards complaints raised by the Commissioner: [named person in SPCB] will review and respond to complaints raised by the Head of Corporate Services, Scottish Information Commissioner
- Where a dispute is unresolved, the Head of Corporate Services may escalate the complaint to the [more senior named person in the SPCB]who shall investigate and respond within 20 working days
- As regards complaints by the DPO: the [Head of Corporate Services] will review and respond to any complaints by the DPO
- Where a dispute is unresolved, the [named person] may escalate the complaint to the Scottish Information Commissioner who shall investigate and respond with 20 working days

8. Role of Commissioner/Ombudsman/Commissions

The Commissioner/Ombudsman/Commissions will:-

- publish contact details of the DPO
- communicate the contact details of the DPO to the relevant supervisory authorities

Deleted: (ICO)

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Comment [LC14]: We should build in something about the DPO returning any information and/or personal data have provided to them in the event that a conflict is identified, including a timescale for return.

Comment [DF15]: This is a first draft indicating the issues that we anticipate will have to be addressed.

Formatted: Font: 11 pt, Underline

Formatted: Indent: Left: 1.27 cm, Right: 0 cm, Line spacing: single, No bullets or numbering

Deleted: Both t

Deleted: and

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Comment [DF16]: It may be useful to set up a process of escalation (ie dealt with at desk level, but ultimately referred to high level for negotiation of settlement).

Comment [DF17]: Should there be a liability clause? How would liability be determined?

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm

Formatted: Font: 11 pt, Underline

Formatted: Font: 11 pt, Underline

Formatted: Font: 11 pt, Underline

- promptly consult with the DPO once a data breach or another incident has occurred
- maintain a record of processing operations under his/her/its responsibility;
- provide the DPO with sufficient information to enable the DPO to accurately relay information to the supervisory authority on how they process personal data. This will ideally be in the form of a flowchart.
- provide the DPO with contact details for his/her office, including out of hours contact details.
- liaise with the DPO to timetable routine meetings, training sessions giving the DPO at least 4 weeks advance notice
- as regards other meetings giving the DPO as reasonable advance notice possible.
- co-operate with the DPO and his/her team
- invite the DPO attend meetings where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;
- give the opinion of the DPO due weight. If there is a disagreement, the reasons for not following the DPO's advice should be documented;
- ensure that if its data processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO will be given the opportunity to make his or her dissenting opinion clear to the Commissioner/Ombudsman/Commissions
- shall seek the DPO's advice when carrying out a DPIA or PIA;
- if they so choose, develop data protection guidelines or programmes that set out when the DPO must be consulted

Deleted: which

Deleted: ICO

Comment [HG18]: If we expect the DPO to be able to contacted "out of hours" we will also need to be provide "out of hours" contact details

Deleted: and other meetings will be arranged as and when required

Formatted: Font: 11 pt

Formatted: Indent: Left: 1.27 cm, Space After: 6 pt, No bullets or numbering

Deleted: to be present

Comment [HG19]: What is meant by this?

Comment [HG20]: Include this?

4.3

Margaret Keyse

From: Helen Gardner-Swift
Sent: 26 March 2018 12:51
To: 'Crerar J (Janice)'
Cc: Turnbull CM (Claire)
Subject: 100302-3 (2018 03 26 Draft MOU for a DPO SIC comments to SPCB)
Attachments: 100302-3 (2018 03 26 Draft MOU for a DPO SIC comments to SPCB).docx

Dear Janice,

Thank you for forwarding the draft MOU to us for comment.

As you are aware, we previously raised concerns about how we could benefit from the shared service proposal taking into account the fact that the proposed DPO will be based within the Scottish Parliament's Information Governance & Management Team. These issues have been considered further and we now think that our concerns can be met by the inclusion of appropriate clauses relating to confidentiality - by ensuring that the DPO acts as an agent and comes within s45 FOISA - and conflicts of interest – by the use of alternative DPO services if a conflict of interest arises which cannot be overcome.

We have also identified that the proposed DPO will need to act as a DPO in respect of our statutory purposes relating to the prevention, investigation, detection or prosecution of criminal offences (see Part 3 DPA 2018). As far as we are aware, we will be the only competent authority amongst the Officeholders who will need a DPO for this purpose.

I have set out on the attached draft of the MOU that you provided suggested amendments and related comments (shown as track changes) relating to the above. I have also included an escalation process for any dispute.

I hope the attached is helpful and I look forward to seeing you on Thursday as I am now able to attend the SPCB GDPR Working Party meeting.

Please let me know if you would like me to forward this email and attachment to the other Officeholder representatives and/or if you need any further information.

Kind regards,

Helen

Helen Gardner-Swift
Head of Corporate Services

Scottish Information Commissioner
Kinburn Castle, Doubledykes Road
St Andrews, KY16 9DS

Tel: 01334 464625
Fax: 01334 464611
Email: hgardnerswift@itspublicknowledge.info
Web: www.itspublicknowledge.info
Twitter: @FOIScotland

Scottish Information Commissioner
it's public knowledge

VC 100302

Memorandum of Understanding

Between

[Commissioner/Ombudsman/Commission]

And

The Scottish Parliamentary Corporate Body

This Memorandum of Understanding is drawn up to provide a basis on which the **officeholder** (henceforward known as the Commissioner/Ombudsman/Commission) and the Scottish Parliamentary Corporate Body (henceforward known as the SPCB) may develop a relationship, specifically for the provision of data protection officer services under the General Data Protection Regulation (the GDPR) that comes into force on 25 May 2018 and the Data Protection Act 2018 [which comes into effect on …] .

1. Background

The General Data Protection Regulation and Data Protection Act 2018 provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the GDPR.

Under the GDPR, it is mandatory for public authorities to designate a DPO.

Under Part 3 of the DPA 2018, it is mandatory for "competent authorities", i.e. authorities which have statutory functions for the purposes of the prevention, investigation, detection or prosecution of criminal offences etc. to designate a DPO for the purpose of those functions.

Both the GDPR and the DPA 2018 lay down conditions for the appointment, position and tasks of the DPO.

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment.

Similarly, Part 3 of the DPA 2018 allows the same person to be designated as a DPO by several controllers.

Under the Shared Services Agenda for officeholders, the SPCB will make available to the [Commissioner/Ombudsman/Commission], at nil cost, a DPO service.

Details of the service to be provided are set out below.

2. General

The SPCB will provide the Commissioner all DPO services, including law enforcement DPO services, as set out in the GDPR and DPA 2018. When carrying out DPO services for the Commissioner, the DPO will be acting as the agent of the Commissioner. Without

Comment [HG1]: Although the DPO will not be party to the DPO there should be a mechanism for the DPO to countersign the MOU as "named DPO" to show their awareness of the terms and functions/duties under the MOU

Deleted: ¶

Deleted: ¶

Deleted: Regulations

Deleted: will

Comment [HG2]: A reference to the Data Protection Act 2018 should also be included

Deleted: s will

Deleted: p

Moved down [1]: The GDPR lays down conditions for the appointment, position and tasks of the DPO.

Comment [HG3]: Referenced "Part 3" only since the final section numbers are not yet known.

Comment [HG4]: Understand that SIC will be the only competent authority which will be signing the MoU.

Moved (insertion) [1]

Deleted: The GDPR

Deleted: s

Deleted: 1998

Deleted: ata Protection Officer

Deleted: Data Protection Act 2018

Comment [HG5]: It is important to include this provision as it brings the DPO under the section 45 of FOISA, which makes it an offence to disclose information obtained (unless the disclosure is made with lawful authority).

prejudice to the foregoing generality, the services provided to the Commissioner will include:-

- A named DPO to attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;
- A DPO to attend, by invitation, such other meetings/working groups dealing with data processing activities:
- To provide advice to the Commissioner/Ombudsman/Commission on matters relating to data protection;
- Provide advice to the Commissioner/Ombudsman/Commission where requested as regards the Data Protection Impact Assessment (DPIA) requirements in Section 3 of the GDPR and Chapter 4 of the DPA 2018 and monitor its performance including (i) whether or not to carry out a DPIA; (ii) what methodology to follow when carrying out a DPIA; (iii) whether to carry out the DPIA in-house or whether to outsource it; (iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; (v) whether or not the DPIA has been correctly carried out and (vi) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR and/or the DPA 2018;
- Inform and advise the [Commissioner/Ombudsman/Commission] and their employees about their obligations to comply with the GDPR, the DPA 2018 and other data protection laws;
- Assist the [Commissioner/Ombudsman/Commission] to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance is set out in paragraph X below;
- Co-operate with the supervisory authority (i.e. the Information Commissioner (ICO)) and act as a contact point for the supervisory authority on issues relating to processing, prior consultation and to consult, where appropriate, with regard to any other matter;
- Act as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and
- The named DPO to be accessible and available to communicate efficiently and clearly with and respond to data subjects (in relation to breach notifications/the right to access/the right to be forgotten).

3. Compliance

The named DPO will not be personally responsible for non-compliance with the GDPR and/or the DPA 2018.

Data protection compliance is the responsibility of the controller or the processor.

The DPO will assist the [Commissioner/Ombudsman/Commission] to monitor compliance by:-

- informing themselves fully of how the [Commissioner/Ombudsman/Commission] processes data ideally through a flowchart;
- advising on DPIAs and Privacy Impact Assessments (PIAs);
- conducting internal audits;
- collecting information to identify processing activities;
- awareness-raising, through training of employees involved in the processing operations, and the related audits;
- providing advice where required as regards DPIAs and monitoring its performance in line with Article 35 of the GDPR/Chapter 4 of the DPA 2018;

Deleted: follows

Deleted: data protection impact assessment

Deleted: ¶

Deleted: body

Deleted: A

Deleted: [

Deleted:]

Deleted: I

Deleted: of equivalent

Deleted: data protection impact assessments

Deleted: the data protection impact assessment

- co-operating with the supervisory authority;
- analysing and checking compliance of processing activities;
- informing, advising and issuing recommendations to the data controller and processor;
- acting as the contact point for the supervisory authority on issues relating to the processing of personal data;
- informing, advising and issuing recommendations to the data controller and processor; and
- being available to employees and data subjects.

Deleted: (ICO)

Deleted: B

4. Accessibility

The named DPO and his/her team will be accessible to the [Commissioner/Ombudsman/Commission] as follows:-

Activity	Timescale
Attend senior management meetings where data protection issues are being discussed	As timetabled
Providing advice on data protection issues	On receipt of all relevant information:- Non urgent - within X working days Urgent – X working days
Training	
Assisting the [Commissioner/Ombudsman/Commission] to determine if there has been a breach	Within X working hours
Assisting the [Commissioner/Ombudsman/Commission] where a data breach or incident has occurred	Be contactable by phone within X hours of the [Commissioner/Ombudsman/Commission] becoming aware that a breach has occurred
Attend such other meetings/working groups dealing with data protection activities	Such reasonable notice as is necessary

Comment [HG6]: Since the notification must be made within 72 hours of becoming aware of the breach, we shouldn't have to wait a number of working days after flagging a potential breach to the DPO for them to provide view on whether there has been a breach.

Deleted: days

Comment [HG7]: This is mentioned in clause 2 and we may want to call in the DPO to attend meetings of the GDPR working party, or meetings about project work which have an impact on our processing of personal data..

Comment [HG8]: There are other activities mentioned in clause 2 which should also have timescales ascribed to them, e.g. acting as contact point with the ICO, or with data subjects about their rights and we would welcome a discussion/suggestions about these

5. Confidentiality

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks for the Commissioner. The Commissioner has specific duties under section 45 of the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (the EIRs) about maintaining confidentiality, and must ensure that his organisation maintains its independence and impartiality, and avoids conflicts of interest. Section 44 of FOISA and regulation 18 of the EIRs also apply to the DPO as agent of the Commissioner. In this context, all information received by the DPO from the Commissioner for the purposes of delivering services to the Commissioner shall be kept confidential and not be disclosed to any third party without the consent of the Commissioner, unless required to be disclosed by law or judicial decree. Third-party is understood to mean any person external to the office of the Scottish Information Commissioner. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.

Deleted: applies

Deleted: (ICO)

6. Conflicts of interest

It is not anticipated that conflicts of interest are likely to arise. However, should any conflict of interest occur, or a situation arise in which it is considered that a conflict of

Comment [HG9]: This is a first draft indicating the issues that we anticipate will have to be addressed.

interest is likely to occur, the DPO should immediately notify the Commissioner and will cease to provide DPO services to the Commissioner in relation to that conflict of interest. The Commissioner will, in such a situation, use alternative DPO services. The DPO will remain bound by the duties of secrecy and confidentiality, including their duties under section 45 of FOISA, in respect of any information obtained by them, as set out in paragraph 5 above.

Comment [HG10]: The DPO should also be required to return any information and/or personal data we have provided to them in the event that a conflict is identified there should be a timescale for return.

7. Complaints and Dispute resolution

The Commissioner ,the SPCB and the DPO shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the MOU within 20 working days of either party notifying the other in writing of the dispute.

Deleted: Both t

Deleted: and

Comment [HG11]: Should there also be a liability clause and, if so, how would liability be determined?

The escalation process for any dispute will be:

- As regards complaints raised by the Commissioner [named person in SPCB] will review and respond to complaints raised by the Head of Corporate Services, Scottish Information Commissioner
- Where a dispute is unresolved, the Head of Corporate Services may escalate the complaint to the [more senior named person in the SPCB] who shall investigate and respond within 20 working days
- As regards complaints by the DPO the [Head of Corporate Services] will review and respond to any complaints by the DPO
- Where a dispute is unresolved, the [named person] may escalate the complaint to the Scottish Information Commissioner who shall investigate and respond with 20 working days

8. Role of Commissioner/Ombudsman/Commissions

The Commissioner/Ombudsman/Commissions will:-

- publish contact details of the DPO
- communicate the contact details of the DPO to the relevant supervisory authorities
- promptly consult with the DPO once a data breach or another incident has occurred
- maintain a record of processing operations under his/her/its responsibility;
- provide the DPO with sufficient information to enable the DPO to accurately relay information to the supervisory authority on how they process personal data. This will ideally be in the form of a flowchart

Deleted: which

Deleted: ICO

- provide the DPO with contact details for his/her office, including out of hours contact details.
- liaise with the DPO to timetable routine meetings, training sessions giving the DPO at least 4 weeks advance notice
- as regards other meetings giving the DPO as reasonable advance notice possible.
- co-operate with the DPO and his/her team
- invite the DPO attend meetings where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;
- give the opinion of the DPO due weight. If there is a disagreement, the reasons for not following the DPO's advice should be documented;
- ensure that if its data processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO will be given the opportunity to make his or her dissenting opinion clear to the Commissioner/Ombudsman/Commissions
- shall seek the DPO's advice when carrying out a DPIA or PIA;
- if they so choose, develop data protection guidelines or programmes that set out when the DPO must be consulted.

Comment [HG12]: The DPO needs to be able to be contacted "out of hours" and, therefore, "out of hours" contact details need to be provided – please let us have these details in due course

Deleted: and other meetings will be arranged as and when required

Deleted: to be present

Comment [HG13]: What is meant by this?

7.4

Memorandum of Understanding

Between

The Scottish Information Commissioner

And

The Scottish Parliamentary Corporate Body

This Memorandum of Understanding is drawn up to provide a basis on which the Scottish Information Commissioner (henceforward known as the Commissioner) and the Scottish Parliamentary Corporate Body (henceforward known as the SPCB) may develop a relationship, specifically for the provision of data protection officer services under the General Data Protection Regulation (the GDPR) that comes into force on 25 May 2018 and the Data Protection Act 2018 [which comes into effect on ...].

1. Background

The General Data Protection Regulation and Data Protection Act 2018 provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the GDPR.

Under the GDPR, it is mandatory for public authorities to designate a DPO.

Under Part 3 of the DPA 2018, it is mandatory for "competent authorities", i.e. authorities which have statutory functions for the purposes of the prevention, investigation, detection or prosecution of criminal offences etc. to designate a DPO for the purpose of those functions.

Both the GDPR and the DPA 2018

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment.

Similarly, Part 3 of the DPA 2018 allows the same person to be designated as a DPO by several controllers.

Under the Shared Services Agenda for parliamentary officeholders, the SPCB will make available to the officeholders, at nil cost, a DPO service.

Details of the service to be provided are set out below.

2. General

The SPCB will provide the Commissioner with DPO services, including law enforcement DPO services, as set out in the GDPR and DPA 2018. When carrying out DPO services for the Commissioner, the DPO will be acting as the agent of the Commissioner. Without prejudice to the foregoing generality, the services provided to the Commissioner will include:-

Comment [JC1]: Discuss - MOU or SLA

Comment [HG2]: Although the DPO will not be party to the DPO there should be a mechanism for the DPO to countersign the MOU as "named DPO" to show their awareness of the terms and functions/duties under the MOU

Deleted: ¶

Comment [HG3]: A reference to the Data Protection Act 2018 should also be included

Moved down [1]:

Comment [HG4]: Referenced "Part 3" only since the final section numbers are not yet known.

Comment [HG5]: Understand that SIC will be the only competent authority which will be signing the MoU.

Moved (insertion) [1]

Comment [HG6]: It is important to include this provision as it brings the DPO under the section 45 of FOISA, which makes it an offence to disclose information obtained (unless the disclosure is made with lawful authority).

VC101189

- A named DPO to attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;
- A DPO to attend, by invitation, such other meetings/working groups dealing with data processing activities:
- To provide advice to the Commissioner on matters relating to data protection;
- Provide advice to the Commissioner where requested as regards the Data Protection Impact Assessment (DPIA) requirements in Section 3 of the GDPR and Chapter 4 of the DPA 2018 and monitor its performance including (i) whether or not to carry out a DPIA; (ii) what methodology to follow when carrying out a DPIA; (iii) whether to carry out the DPIA in-house or whether to outsource it; (iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; (v) whether or not the DPIA has been correctly carried out and (vi) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR and/or the DPA 2018;
- Inform and advise the Commissioner and their employees about their obligations to comply with the GDPR, the DPA 2018 and other data protection laws;
- Assist the Commissioner to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance is set out in paragraph X below;
- Co-operate with the supervisory authority, i.e. the Information Commissioner (ICO) and act as a contact point for the supervisory authority on issues relating to processing, prior consultation and to consult, where appropriate, with regard to any other matter;
- Act as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and
- The named DPO to be accessible and available to communicate (efficiently and clearly) with and respond to data subjects in relation to breach notifications/the right to access/the right to be forgotten).

3. Compliance

The named DPO will not be personally responsible for non-compliance with the GDPR and/or the DPA 2018.

Data protection compliance is the responsibility of the controller or the processor.

The DPO will assist the Commissioner to monitor compliance by:-

- informing themselves fully of how the Commissioner processes data ideally through a flowchart;
- advising on DPIAs and Privacy Impact Assessments (PIAs);
- conducting internal audits;
- providing an annual assurance report;
- collecting information to identify processing activities;
- awareness-raising, through training of employees involved in the processing operations, and the related audits;
- providing advice where required as regards DPIAs and monitoring its performance in line with Article 35 of the GDPR/Chapter 4 of the DPA 2018;
- co-operating with the supervisory authority;
- analysing and checking compliance of processing activities;
- informing, advising and issuing recommendations to the data controller and processor;

Deleted: ¶

Deleted: .

Deleted: I

Deleted: of equivalent

Deleted: data protection impact assessments

Deleted: ;

Deleted: the data protection impact assessment

Deleted: (ICO)

- acting as the contact point for the supervisory authority on issues relating to the processing of personal data;
- informing, advising and issuing recommendations to the data controller and processor; and
- being available to employees and data subjects.

4. Accessibility

The DPO and her team can be contacted as follows:-

Named DPO	Tel (office hours): 0131 348 Mobile: Email:
DPO Team	Tel (office hours): Mobile: email

The named DPO and her team will be accessible to the Commissioner as follows:-

Activity	Contact options	Timescale
Attend senior management meetings where data protection issues are being discussed		As timetabled
Providing advice on data protection issues	Telephone or email	On receipt of all relevant information:- Non urgent – within X working days as agreed Urgent – within X hours of contacting the DPO Team
Training	Requests for training should be made via the DPO Team	As agreed but within X weeks/months of the request
Assisting the Commissioner to determine if there has been a breach	Telephone, conference call or email	Within X working hours
Assisting the Commissioner where a data breach or incident has occurred	Telephone, conference call or email	Be contactable by phone within X hours of the Commissioner becoming aware that a breach has occurred
Attend such other meetings/working groups dealing with data protection activities	Requests for DPO to attend meetings etc should be made via the DPO Team	Such reasonable notice as is necessary

Comment [HG7]: Since the notification must be made within 72 hours of becoming aware of the breach, we shouldn't have to wait a number of working days after flagging a potential breach to the DPO for them to provide view on whether there has been a breach.

Comment [HG8]: This is mentioned in clause 2 and we may want to call in the DPO to attend meetings of the GDPR working party, or meetings about project work which have an impact on our processing of personal data..

5. Confidentiality

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks for the Commissioner. The Commissioner has specific duties under section 45 of the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (the EIRs) about maintaining confidentiality, and must ensure

that his organisation maintains its independence and impartiality, and avoids conflicts of interest. Section 45 of FOISA and regulation 18 of the EIRs also apply to the DPO as agent of the Commissioner. In this context, all information received by the DPO from the Commissioner for the purposes of delivering services to the Commissioner shall be kept confidential and not be disclosed to any third party without the consent of the Commissioner, unless required to be disclosed by law or judicial decree. Third-party is understood to mean any person external to the office of the Scottish Information Commissioner. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.

Deleted: applies

Deleted: .

Deleted: (ICO)

6. Conflicts of interest

It is not anticipated that conflicts of interest are likely to arise. However, should any conflict of interest occur, or a situation arise in which it is considered that a conflict of interest is likely to occur, the DPO should immediately inform the Commissioner and will cease to provide DPO services to the Commissioner in relation to that conflict of interest. The Commissioner will, in such a situation, use alternative DPO services. The DPO will remain bound by the duties of secrecy and confidentiality, including their duties under section 45 of FOISA, in respect of any information obtained by them, as set out in paragraph 5 above.

Comment [HG9]: This is a first draft indicating the issues that we anticipate will have to be addressed.

Comment [HG10]: The DPO should also be required to return any information and/or personal data we have provided to them in the event that a conflict is identified there should be a timescale for return.

7. Complaints and Dispute resolution

The Commissioner, the SPCB and the DPO shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the MOU within 20 working days of either party notifying the other in writing of the dispute.

Deleted: Both t

Deleted: and

Comment [HG11]: Should there be a also be a liability clause and, if so, how would liability be determined?

The escalation process for any dispute will be:

- As regards complaints raised by the Commissioner: [named person in SPCB] will review and respond to complaints raised by the Head of Corporate Services, Scottish Information Commissioner
- Where a dispute is unresolved, the Head of Corporate Services may escalate the complaint to the [more senior named person in the SPCB] who shall investigate and respond within 20 working days
- As regards complaints by the DPO: the [Head of Corporate Services] will review and respond to any complaints by the DPO
- Where a dispute is unresolved, the [named person] may escalate the complaint to the Scottish Information Commissioner who shall investigate and respond with 20 working days

8. Role of Commissioner

The Commissioner will:-

- publish contact details of the DPO
- communicate the contact details of the DPO to the relevant supervisory authorities
- promptly consult with the DPO once a data breach or another incident has occurred
- maintain a record of processing operations under his/her/its responsibility;
- provide the DPO with sufficient information to enable the DPO to accurately relay information to the supervisory authority on how they process personal data. This will ideally be in the form of a flowchart.
- provide the DPO with contact details for his/her office, including out of hours contact details.
- liaise with the DPO to timetable routine meetings, training sessions giving the DPO at least 4 weeks advance notice.
- as regards other meetings giving the DPO as reasonable advance notice possible.
- co-operate with the DPO and his/her team
- invite the DPO to attend meetings where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;
- give the opinion of the DPO due weight. Provide an opportunity for the DPO to make his/her dissenting opinion clear to those making the decisions and if there is a disagreement, the reasons for not following the DPO's advice should be documented;
- shall seek the DPO's advice when carrying out a DPIA or PIA;
- if they so choose, develop data protection guidelines or programmes that set out when the DPO must be consulted

9. Review mechanism

The services outlined in and operation of this SLA will be reviewed after one year. Both parties will meet to consider where the SLA worked well and identify any issues. The aim of the review is to resolve any issues and embed good practice. If required, the SLA will be amended. If both parties cannot agree, the dispute resolution process will come into effect. After the initial review, either party may request a review of the SLA as and when required.

10. Termination

Comment [HG12]: The DPO needs to be able to be contacted "out of hours" and, therefore, "out of hours" contact details need to be provided – please let us have these details in due course

Deleted: and other meetings will be arranged as and when required

Deleted: .

Deleted: to be present

Either party may terminate this agreement on giving xx working days' notice in writing. The dispute resolution process must be exhausted prior to a termination notice being issued. [The notice period should allow enough time for the SPCB to allocate other work to their DPO (if terminated by office-holder) or for Office-holder to find suitable alternative DPO (if terminated by SPCB)].

7~

Scottish Information Commissioner
www.itspublicknowledge.info

Service Level Agreement

between

The Scottish Information Commissioner

and

The Scottish Parliamentary Corporate Body

This Service Level Agreement~~Memorandum of Understanding~~ (SLA) is drawn up to provide a basis on which the Scottish Information Commissioner (henceforward known as the Commissioner) and the Scottish Parliamentary Corporate Body (henceforward known as the SPCB) may develop a relationship, specifically for the provision of data protection officer services, under the General Data Protection Regulation (the GDPR) that comes into force on 25 May 2018 and the Data Protection Act 2018 (the DPA 2018) which is due to come into effect in May 2018.

Background

1. The GDPR and the DPA 2018 provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the legislation.

2. Under the GDPR, it is mandatory for public authorities to designate a DPO.

3. Under Part 3 of the DPA 2018, it is mandatory for "competent authorities", i.e. authorities which have statutory functions for the purpose of the prevention, investigation, detection of prosecution of criminal offences, etc. to designate a DPO for the purpose of those functions. The Commissioner is a competent authority for the purposes of Part 3 of the DPA 2018.

4. Article 37(2) of the GDPR allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment.

~~4.~~5. Similarly, Part 3 of the DPA 2018 allows the same person to be designated as a DPO by several controllers.

~~5.~~6. Under the Shared Services Agenda for parliamentary officeholders, the SPCB will make available to the ~~officeholders~~Commissioner, at nil cost, a DPO service.

6.7. Details of the service to be provided, at nil cost, are set out below.

General

7.8. The SPCB will provide the Commissioner with DPO services from a named DPO, including law enforcement DPO services, as set out in the GDPR and the DPA 2018. When carrying out the DPO services for the Commissioner, the DPO will be acting as the agent of the Commissioner. Without prejudice to the foregoing generality, the services provided to the Commissioner will include:

(i) A named DPO to attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;

(ii) A DPO to attend, by invitation, such other meetings/working groups dealing with data processing activities;

(iii) Providing advice to the Commissioner on matters relating to data protection;

(iv) Providing advice to the Commissioner where requested as regards the Data Protection Impact Assessment (DPIA) requirements in Section 3 of the GDPR and Chapter 4 of the DPA 2018 and monitoring its performance including:

(a) whether or not to carry out a DPIA;

(b) what methodology to follow when carrying out a DPIA;

(c) whether to carry out the DPIA in-house or whether to outsource it;

(d) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;

(e) whether or not the DPIA has been correctly carried out and

(f) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR and/or the DPA 2018;

(v) Informing and advising the Commissioner and his employees about their obligations to comply with the GDPR, the DPA 2018 and other data protection laws;

~~(iv)~~(vi) Assisting the Commissioner to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance are set out in paragraph 12 below;

~~(v)~~(vii) Co-operating with the supervisory authority, i.e. the Information Commissioner (ICO) and acting as a contact point for the supervisory authority on issues relating to processing, ~~prior consultation~~ and ~~to~~ consulting with the supervisory authority, where appropriate, with regard to any other relevant matter;

~~(vi)~~(viii) Acting as a contact point to facilitate access by the supervisory authority to documents and information for the performance of its tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and

~~(vii)~~(ix) The named DPO being accessible and available to communicate (efficiently and clearly) with and respond to data subjects in relation to breach notifications/the right to access/the right to be forgotten).

Compliance

~~8.~~9. The named DPO will not be personally responsible for non-compliance with the GDPR and/or the DPA 2018.

~~9.~~10. Data protection compliance is the responsibility of the controller or the processor.

~~10.~~11. The DPO will assist the Commissioner to monitor compliance by:

(i) informing themselves fully of how the Commissioner processes data ideally through a flowchart ~~of equivalent~~;

(ii) advising on DPIAs and Privacy Impact Assessments (PIAs);

(iii) conducting internal audits;

(iv) providing an annual assurance report;

(v) collecting information to identify processing activities;

(vi) awareness-raising, through training of employees involved in the processing operations, and the related audits;

(vii) providing advice where required as regards DPIAs and monitoring his performance in line with Article 35 of the GDPR/Chapter 4 of the DPA 2018;

(viii) co-operating with the supervisory authority;

(ix) analysing and checking compliance of processing activities;

(x) informing, advising and issuing recommendations to the data controller and processor;

(xi) acting as the contact point for the supervisory authority on issues relating to the processing of personal data;

(xii) informing, advising and issuing recommendations to the data controller and processor; and

(xiii) being available to employees and data subjects.

Accessibility

~~11.~~ 12. The DPO and her team can be contacted as follows:-

Comment [MK1]: Details to be completed.

Named DPO	Tel (office hours): 0131 348 Mobile: Email:
DPO Team	Tel (office hours): Mobile: email

~~12.~~ 13. The named DPO and her team will be accessible to the Commissioner as follows:-

Comment [MK2]: Details to be completed.

Activity	Contact options	Timescale
Attend senior management meetings where data protection issues are being discussed		As timetabled
Providing advice on data protection issues	Telephone or email	On receipt of all relevant information:- Non urgent – within X working days as agreed Urgent – within X hours of contacting the DPO Team
Training	Requests for training should be made via the DPO Team	As agreed but within X weeks/months of the request
Assisting the Commissioner to determine if there has been a breach	Telephone, conference call or email	Within X working hours
Assisting the Commissioner where a data breach or incident has occurred	Telephone, conference call or email	Be contactable by phone within X hours of the Commissioner becoming aware that a breach has occurred
Attend such other meetings/working groups dealing with data protection activities	Requests for DPO to attend meetings etc should be made via the DPO Team	Such reasonable notice as is necessary

Confidentiality

~~13.~~ 14. The DPO is bound by secrecy or confidentiality concerning the performance of his ~~or her~~ tasks for the Commissioner. The Commissioner has specific duties under section 45 of the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (the EIRs) about maintaining confidentiality, and must ensure that his organisation maintains its independence and impartiality, and avoids conflicts of interest. Section 45 of FOISA and regulation 18 of the EIRs also apply to the DPO as agent of the Commissioner. In this context, all information received by the DPO from the Commissioner for the purposes of delivering services to the Commissioner shall be kept confidential and not be

disclosed to any third party without the consent of the Commissioner, unless required to be disclosed by law or judicial decree. Third-party is understood to mean any person external to the office of the Scottish Information Commissioner. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.

Conflicts of interest

~~14.~~15. It is not anticipated that conflicts of interest are likely to arise. However, should any conflict of interest occur, or a situation arise in which it is considered that a conflict of interest is likely to occur, the DPO should immediately notify the Commissioner and will cease to provide DPO services to the Commissioner in relation to that conflict of interest. The Commissioner will, in such a situation, use alternative DPO services. The DPO will remain bound by the duties of secrecy and confidentiality, including their duties under section 45 of FOISA, in respect of any information obtained by them, as set out in paragraph 14 above. The DPO will also undertake to return any information and/or personal data the Commissioner has provided to her within X working days.

Comment [MK3]: To be completed.

Complaints and Dispute resolution

~~15.~~16. The Commissioner, the SPCB and the DPO shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with this SLA within 20 working days of either party notifying the other in writing of the dispute.

Comment [HG4]: Should there be a also be a liability clause and, if so, how would liability be determined?

~~16.~~17. The escalation process for any dispute will be:

(i) As regards complaints raised by the Commissioner: [named person in SPCB] will review and respond to complaints raised by the Head of Corporate Services, Scottish Information Commissioner

Comment [MK5]: To be completed.

(ii) Where a dispute is unresolved, the Head of Corporate Services may escalate the complaint to the [more senior named person in the SPCB] who shall investigate and respond within 20 working days

Comment [MK6]: To be completed.

(iii) As regards complaints by the DPO: the Head of Corporate Services will review and respond to any complaints by the DPO

(iv) Where a dispute is unresolved, the [named person] may escalate the complaint to the ~~Scottish Information~~ Commissioner who shall investigate and respond with 20 working days

Comment [MK7]: To be completed

Role of Commissioner

~~17.~~18. The Commissioner will:

(i) publish contact details of the DPO;

(ii) communicate the contact details of the DPO to the relevant supervisory authority;

(iii) promptly consult with the DPO once a data breach or another incident has occurred;

(iv) maintain a record of processing operations under his/her/its responsibility;

(v) provide the DPO with sufficient information to enable the DPO to accurately relay information to the supervisory authority on how he processes personal data. This will ideally be in the form of a flowchart;

(vi) provide the DPO with contact details for his office, including out of hours contact details;

Comment [HG8]: The DPO needs to be able to be contacted "out of hours" and, therefore, "out of hours" contact details need to be provided – please let us have these details in due course

(vii) liaise with the DPO to timetable routine meetings and, training sessions, giving the DPO at least 4 weeks' advance notice;

(viii) liaise with the DPO as regards other meetings, giving the DPO as reasonable advance notice possible;

(ix) co-operate with the DPO and his/her team;

(x) invite the DPO to attend meetings where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

(xi) give the opinion of the DPO due weight;

(xii) provide an opportunity for the DPO to make his/her dissenting opinion clear to those making the decisions and, if there is a disagreement, document the reasons for not following the DPO's advice should be documented;

(xiii) shall seek the DPO's advice when carrying out a DPIA or PIA;

(xiv) if he so chooses, develop data protection guidelines or programmes that set out when the DPO must be consulted.

Commencement date

19. Regardless of the date or dates of the signing of this SLA, the SLA shall take effect from 25 May 2018.

Review mechanism

18. The services outlined in and operation of this SLA will be reviewed within one year of its commencement. Both parties will meet to consider where the SLA worked well and identify any issues. The aim of the review is to resolve any issues and embed good practice. If required, the SLA will be amended. If both parties cannot agree, the dispute resolution process will come into effect. After the initial review, either party may request a review of the SLA as and when required.

Formatted: Normal, Indent: Left: 0.63 cm, Hanging: 0.63 cm, No bullets or numbering

Termination

19. Either party may terminate this agreement on giving xx working days' notice in writing. The dispute resolution process must be exhausted prior to a termination notice being issued. ~~[The notice period should allow enough time for the SPCB to allocate other work to their DPO (if terminated by office-holder) or for Office-holder to find suitable alternative DPO (if terminated by SPCB)].~~

Comment [MK9]: To be completed.

..... Date .....

Scottish Information Commissioner

..... Date .....

Scottish Parliamentary Corporate Body

..... Date .....

Data Protection Officer