

LMS Data Protection Compliance Guide

Introduction

1. The Data Protection Act (DPA) 1998 put in place legislation to protect the rights of individuals in terms of the data (both electronic and clerical) held on them. The DPA sets out safeguards for the processing of personal data, which acts as a framework governing how we collect data, what we do with it, who we give it to and the access of individuals to that data.
2. This means we must ensure that we have a legal basis for collecting customer information and tell the customer why we are collecting it and what we do with it.

Data Protection Principles

3. The Act details eight “Data Protection Principles” that must be followed on how personal data must be processed both on IT systems and on paper. We need to make sure that all personal data held on our systems is:
 - fairly and lawfully processed;
 - processed for limited purposes;
 - adequate, relevant and not excessive;
 - accurate and up to date;
 - not kept for longer than is necessary;
 - processed in line with an individual’s rights;
 - secure; and
 - not transferred to countries that do not have adequate protection.

Recording Sensitive Personal Information for Benefit Customers

Introduction

4. Social Security legislation provides authority for Jobcentre Plus to gather the basic information that is required to apply for the DWP benefit claimed by the customer. We can only record additional information if the customer fully understands how we will use it and gives us their consent to do so.

Sensitive Personal Data

5. The DPA attaches extra safeguards to the processing of ‘Sensitive Personal Data’ but sensitive data can be processed where the data subject has given their **explicit** consent, providing the data processing is required to enable the Department to carry out its functions.

Recording Sensitive Information on LMS

6. In order to comply with the DPA we must obtain the customer's freely given, fully informed and explicit consent to record sensitive information on LMS. We do this by ensuring that the consent form DPA1 is completed. The DPA1 form can be obtained from the Zanzibar catalogue. In addition consent to record ethnicity or refugee status is obtained using the Ensuring Equality for All (EEA5JP) leaflet (see also paragraphs 16 and 17).

7. Sensitive information is often sought to support our current business processes and to help make sure we provide people with appropriate services; e.g. to confirm eligibility to access early entry to a Jobcentre Plus provision.

8. The categories of sensitive information under DPA are:

- health or physical condition
- race/ethnic origin
- sexual life
- religious beliefs
- trade union membership
- any offence committed by them
- any court proceedings against them

9. We can use markers on LMS to record whether a customer is:

- Currently serving a community sentence, custodial sentence or is an ex-offender
- A current/recovering/stabilised drug mis-user
- A recovering/stabilised alcoholic
- Has a health problem or disability affecting their day-to-day activities.

10. The use of these markers, or storing similarly sensitive information in conversations, is regarded as the processing of sensitive information and can only be recorded on LMS when the DPA1 has been completed and signed by the customer.

11. The consent will remain valid while the claim remains live, unless the customer requests that the details be removed.

12. If a claim becomes inactive, the consent will remain valid for up to 13 weeks. If a customer returns to make another claim within the 13-week period, you must check that the information held on the system is still relevant. If the information is still relevant, a new DPA1 is not required. However, a new DPA1 must be completed for a claim made after this 13-week period.

13. The 'Other' category on the DPA1 allows users to record in LMS conversations sensitive information related to sex, religious beliefs and trade union membership that a customer considers sensitive but for which no LMS marker is held.

Obtaining Retrospective Consent

14. Where sensitive data was recorded on LMS prior to the introduction of this guidance, retrospective consent must be obtained at the customer's next intervention using the DPA1.

Telephone Contact

15. If a customer discloses sensitive information over the telephone we may obtain **interim** verbal confirmation. However, the customer **must** complete a DPA1 when they next attend the office. When verbal consent has been obtained, make a note in LMS conversations. Subsequently, when the customer next attends, record the date that the DPA 1 was completed.

EEA5JP – Ensuring Equality for All

16. We already seek consent to record information about ethnicity status and the customer's health condition on the EEA5JP and we can continue to hold this information without the customer having to complete the DPA1. However, this information can only be stored for the purposes specified in the EEA5JP leaflet.

17. Therefore, if sensitive information is going to be used for anything over and above this, such as early entry to provision due to ethnicity, further consent must be obtained using the DPA1. When the customer has completed the DPA1, the sensitive details can be input to LMS.

What happens to the DPA1 Form?

18. The Data Protection Act also covers the security of sensitive information stored clerically e.g. information held in the Labour Market Unit (LMU). As there is no audit trail for accessing clerical records, we must not store any sensitive information in a customer's LMU/case papers or similar documentation. Therefore, once the details have been entered in the 'Client Record' on LMS, the tear-off part of the consent form must be destroyed. However, the signed declaration part of the DPA1 can be retained in the LMU/case papers or similar documentation.

19. The only instance where the entire DPA1 can be stored in the LMU is where the customer's record is being treated as sensitive and the customer's details are held in a secure cabinet. Please note: Sensitive records must remain locked in secure filing cabinets at all times -see Chapter B of the LMS User Guide for further details.

20. The customer's signed declaration will remain on file until the claim becomes dormant. Once dormant the DPA1 form will be purged along the same retention periods as the LMU or equivalent.

Customer chooses not to give consent

21. If a customer chooses not to give their consent then any details referring to the sensitive information cannot be recorded on LMS.

22. If sensitive information is already held on the system, then any references to this must be removed. Before making any changes to the record you must first seek clearance from your business manager.

23. Following agreement from your business manager, any fields/indicators that contain sensitive information must be amended/re-set to ensure that all traces of the sensitive information have been removed.

24. In instances where the customer record needs to remain but the data that needs removing cannot be removed locally, you will need email DWP OITC Team to arrange for the details to be removed. To do this, follow the step actions in paragraphs 51 to 54 of this guide.

25. Any details about the customer's ethnicity/refugee status that are contained behind the ethnicity marker may remain, as the customer will have already consented to this by completing the EEA5JP.

26. Where sensitive information is stored that is relevant to the benefit the customer is claiming (e.g. the DP marker is set because the customer is claiming Incapacity Benefit) then these details can also remain.

27. In instances where a customer chooses not to provide consent but still wishes to enter a Jobcentre Plus programme early you cannot refuse access. In these instances, Jobcentre Plus staff will need to record the referral on LMS under the 'Adviser Discretion' category on the drop down menu for recording early entry. A note must also be made in LMS conversations to say that early entry has been permitted at the Adviser's Discretion.

Recording Personal Information for Non-Benefit Customers

28. In order to measure Jobcentre Plus performance against the Job Outcome Target, data from the Department for Work and Pensions benefit systems and Labour Market System are fed into the Work and Pensions Longitudinal Study (WPLS). Employment data (P45 and P46 details) from Her Majesty's Revenue and Customs are also passed to WPLS to match against our customer data. Therefore, customers must be made aware of this.

29. Customers who are claiming a work-related benefit are made aware of how we will use their personal details through:

- the DWP confidentiality statement included on benefit claim forms;
- through the Privacy Policy on the DWP website.

However, non-benefit customers may not be aware of how we will use their personal details and therefore need to be asked if an LMS customer record can be created to store their personal details.

30. When creating a new record for a non-benefit customer, you must explain to them that we need their permission to record their personal details on our computer system and the reason why we need to do so.

31. All staff that deal with non-benefit customers looking for work must seek customer consent by using the following script:

To comply with the Data Protection Act we need your permission to store information about you on our computer systems. We use this information to help with research and statistical purposes only. To help with this we measure job outcomes by linking your details with employment information that we receive from Her Majesty's Revenue and Customs.

Are you happy for us to record your personal details on our computer systems for these purposes?

32. If the customer asks for further information about this please refer to the Question and Answer Brief

33. If the customer provides consent, you must hand them, or post them, form DPA2 - Storing your personal information, which will further explain why we hold their details. This form is currently only available as an Appendix to this chapter. You must then make a note in LMS conversations that verbal consent has been obtained and the DPA2 has been issued accordingly.

34. Customers who have an existing record may not previously have been given an explanation about DPA or why we have recorded their details on our system. In these circumstances, you must check the customer's record to see if a note regarding the issue of a DPA2 has been made in LMS conversations. If a note has not been made, you must explain to the customer why we need to record their personal details, send or post them a DPA2 and make a note to that effect in LMS conversations.

What happens if a customer refuses to give their consent?

35. We cannot refuse to help customers who (after being told why we want to record their details on our database) are unwilling to give us their consent. When a customer refuses to give consent, details must not be recorded on LMS.

36. Quite often non-benefit customers will also disclose information of a sensitive nature such as:

- They are an ex-offender
- They have a health problem or disability
- They are a current/recovering/stabilised drug mis-user
- They are a recovering/stabilised alcoholic
- They are a refugee

37. For instances such as these the best form of consent is always in writing so that there is supporting evidence should the business be challenged under the Data Protection Act. Therefore, wherever possible (for example: during outreach work, prison liaison work or jobsfairs when you are seeing the customer face-to-face) you should obtain consent on the DPA1 form. The return part of the form must then be kept in a secure cabinet.

38. However, it is not possible to obtain written consent from non-benefit customers who disclose sensitive information via our Jobcentre Plus Direct services.

39. Because calls to Jobcentre Plus Direct are recorded and retained and will therefore provide the supporting evidence required should we face a DPA challenge, we can accept verbal consent in these instances.

40. Therefore, in addition to asking the customer whether we can record their personal details we also need to ask for permission to store sensitive information about them as well. Jobcentre Plus Direct will need to introduce a script on the lines of:

'You have disclosed that you are/have [insert details of sensitive information – e.g. a health problem or disability]

41. If the customer agrees, the relevant marker(s) should be set. However, if a customer refuses, you must not set any marker or record the sensitive information anywhere on LMS.

42. Any other telephone contacts are not recorded so if sensitive information is disclosed during these calls you must not set any markers or record this information on LMS.

43. Copies of the DPA1 form can be obtained from the Zanzibar catalogue.

44. Where sensitive data was recorded on LMS prior to the introduction of this guidance, retrospective consent must be obtained from the customer and a note must be made in LMS conversations that retrospective consent has been obtained.

Customer requests that their details are removed from LMS

45. If after receiving a copy of the DPA2 a customer requests for their details to be removed you must take immediate action to do this.

46. However, if prior to becoming a non-benefit customer there are details held on LMS relating to a previous claim to benefit and this period is still within 14 months of the end of the claim, the customer must be told that these details will need to remain for audit purposes as determined by policy.

47. In instances where an on-going fraud investigation is being undertaken, you cannot do anything to jeopardise this and must NOT remove any evidence linked to this investigation

48. It is not possible to completely delete a client record from LMS. Therefore, all personal information that can identify a customer must be removed / amended on the client record so that we meet the obligations under the Data Protection Act. To do this you will need to:

Step	Action
1	Open the relevant client record
2	Click on [Amnd];
3	Set the Employment Status [Emp Stat] field to 'Not Known'
4	Set the [Status] field to 'Inactive'
5	Overtyping the Surname and Forename fields with DELETED
6	Amend the 'Date of Birth' (DOB) field to 01/01/1901.
7	Delete the National Insurance Number, Address and Telephone Number fields.

8	Click on [Save] to update the revised record. When saving the details LMS will recognise the person to be over 65 years old and you will need to confirm that this is correct.
---	--

Customer does not provide retrospective consent to store their details and/or sensitive information

49. When trying to obtain retrospective consent the customer may decide that they do not want their details to remain on LMS. In these instances you must take immediate action to remove the customer's details by following the steps indicated in paragraphs 45 to 48 and inform the customer that steps are being taken to remove their details.

50. In instances where a customer is happy for their personal details to remain on LMS but no longer wishes for any sensitive data to be stored you must take immediate steps to remove this data from LMS.

51. Where the customer record can be amended locally, i.e. markers can be unset or conversations amended you must seek approval from your business/contact centre manager (or nominated officer of Band E or above) before making any changes to the customer record.

52. In instances where the customer record needs to remain but the data that needs removing cannot be removed locally, you will need to email DWP OITC Team to arrange for the details to be removed. To do this follow the step actions below:

Step	Action
1	Electronically complete parts 1, 2 and 3 of the DPA3 form – Request to remove client details on LMS
2	Forward the completed form to your Business/Contact Centre Manager (or nominated person at Band E or above) to complete part 4.
3	Nominated person to complete part 4 of the form and electronically save it to a secure folder. The completed version of the form must be saved for 12 months for audit purposes.
4	Nominated person to e-mail the completed DPA3 to DWP OITC Team.
5	DWP OITC Team will investigate your request and any genuine request to remove data from a customer record will incur a cost. You will be asked to provide a Cost Centre number in order for this work to be carried out. The DWP OITC Team will contact you once the request has been carried out to ask you to check that the amendments to the customer record are correct.

Jobsfairs, Open Days, Large Scale Recruitments or Large Scale Redundancies

Benefit Customers

53. If you are taking part in these events you must ensure that you obtain consent from any customers who disclose information of a sensitive nature as we may wish to record details onto LMS at a later date. You must therefore ensure that you carry stocks of the DPA1.

54. Before obtaining consent from these customers you must identify yourself as a Jobcentre Plus employee and explain that any details of a sensitive nature that the customer has provided will be input to LMS.

55. If the customer requests that we do not store their sensitive information, either on LMS or clerically, you must not record these.

Non-Benefit Customers

56. If you are taking part in these events you must ensure that you obtain consent from non-benefit customers allowing you to gather and record their personal information.

57. You must identify yourself as a Jobcentre Plus employee and explain that the details they provide will be input to DWP computer systems and used to help them in their search for work and for performance purposes only. You must also ensure that customers are given a DPA2, which explains in more detail about what we do with their data.

58. If however, the customer requests that we do not store their details, either on LMS or clerically, you must not record any information of this nature but continue to refer/submit these customers to jobs.

Non-benefit Customers Q&A Brief

Q Why do you need to store my personal details on your computer systems?

A By storing basic personal information about you, such as your address and contact details it helps us when trying to contact you.

Q Are your computer systems secure?

A All our computer systems can only be accessed by staff working for the Department for Work and Pensions (DWP) and meet with current legislation (Data Protection Act 1998) about storing personal information about customers. All systems are also subject to robust audit trails.

Q What do you do with my personal details if I stop using your services to find work?

A Individual customer records that have not been accessed for a period of time are made inactive and purged from the system through the automated purge processes we have in place. A copy of the data used for research and statistics

only is stored separately and held for longer, but access is very strictly controlled.

Q Is my personal information shared with any third parties?

A We will only share your information with prospective employers and other organisations that are contracted to DWP to provide training opportunities or provision that helps you to find employment but this will only be by pre-arrangement with yourself.

Q What else do you use my personal information for?

A When we set up your personal customer record on our labour market system – this information is automatically transferred to the Work and Pensions Longitudinal Study (WPLS). This system is owned by DWP and is used for a range of research and statistical purposes. Employment data from Her Majesty's Revenue and Customs (HMRC) are also fed into WPLS so that Jobcentre Plus can measure job outcomes. This means that when you find a job WPLS will automatically match your details with this employment data and record a job outcome. The data provided on job outcomes is anonymous and individual's details are not attached to this. HMRC do not have access to WPLS.

Q What happens if I refuse to let you store my details?

A We will not store any information about you but we will continue to help you in your search for work where we can. It may take longer to help you find suitable employment because we cannot search for jobs using any criteria provided by you which means that some jobs we find are not an exact match to the type of work you are looking for. This will also mean that Jobcentre Plus cannot monitor how instrumental it has been in helping you find a job because your details will not be present on our systems. This will affect our ability to understand how our services work overall and so reduce our ability to make improvements.

Q I am in receipt of Tax Credits and Child Benefit – will refusing to let you store my details affect this?

A Any benefits you are receiving will not be affected if you refuse consent. The information we require about you is purely for research and analytical purposes only.

DPA1W – Ffurflen Ganiatâd

| This is the latest Welsh version of the DPA1W form. Please note that printed versions of this form are not available from the Zanzibar catalogue.

DPA1 Consent Form

| This is the latest version of the DPA1 form.

DPA 2: Storing your personal information

You have provided verbal consent to allow Jobcentre Plus to store your personal information on our computer systems. This form provides you with further details about how your information is processed and used.

The information that you have provided is stored on our Labour Market System (LMS). LMS is the computer system used in Jobcentre Plus, part of the Department for Work and Pensions (DWP), that holds details of customer personal information and opportunities provided by suppliers of training and work-based learning initiatives. Only DWP staff have access to LMS.

As well as recording your personal information on LMS we will also record details of any interviews or contact with us you have had and any training initiatives that you have been referred to.

Also, Jobcentre Plus needs information about the numbers of customers we help into work so that we can measure our performance and improve the services we provide. To help us do this, Her Majesty's Revenue and Customs (HMRC) provides us with employment data (completed P45 – Details of Employee Leaving Work / P46 - PAYE Notice of New Employee form), which we combine with the data we already hold to produce information about job outcomes. This is done in a very strictly controlled and secure way and it will not affect the services you receive from either DWP or HMRC.

You have the right to withdraw your consent at any time. Where you choose to do this you will need to contact Jobcentre Plus, preferably in writing, to ask them to remove your details from LMS.

For more information on the Data Protection Act access the data protection page at www.dwp.gov.uk/privacy-policy.

DPA 2W: Cadw eich gwybodaeth bersonol

Rydych wedi rhoi caniatâd ar lafar sy'n caniatáu'r Ganolfan Byd Gwaith gadw eich gwybodaeth bersonol ar ein systemau cyfrifiadurol. Mae'r ffurflen hon yn rhoi rhagor o wybodaeth i chi am sut y caiff y wybodaeth ei phrosesu a'i defnyddio.

Cedwir y wybodaeth a roddwyd gennych ar ein System Marchnad Lafur (LMS). System gyfrifiadurol yw'r LMS a ddefnyddir gan y Ganolfan Byd Gwaith, rhan o'r Adran Gwaith a Phensiynau (DWP), sy'n cadw manylion gwybodaeth bersonol cwsmeriaid a chyfleoedd a ddarparwyd gan ddarparwyr hyfforddiant a mentrau sy'n seiliedig ar waith. Dim ond staff DWP sydd â mynediad i LMS.

Yn ogystal â chofnodi eich gwybodaeth bersonol ar LMS byddwn hefyd yn cofnodi manylion unrhyw gyfweiliad neu gysylltiad â ni ac unrhyw fentrau hyfforddiant rydych wedi cael eich cyfeirio atynt.

Mae'r Ganolfan Byd Gwaith hefyd angen gwybodaeth am niferoedd y cwsmeriaid rydym yn eu helpu i mewn i waith er mwyn i ni allu mesur ein perfformiad a gwella'r gwasanaethau a ddarparwn. I'n helpu i gyflawni hyn, mae Cyllid a Thollau EM (HMRC) (Cyllid y Wlad yn flaenorol) yn rhoi data cyflogaeth i ni (P45 wedi'i gwblhau –Manylion Cyflogai'n gadael Gwaith / P46 – Ffurflen PAYE Hysbysiad o Gyflogai Newydd), yr ydym yn ei gyfuno gyda'r data sydd eisoes gennym i gynhyrchu gwybodaeth am ganlyniadau swyddi. Gwneir hyn mewn ffordd a reolwyd yn llym ac yn ddiogel ac ni fydd yn effeithio ar y gwasanaethau a gewch gan un ai DWP neu HMRC.

Mae gennych yr hawl i dynnu'ch caniatâd yn ôl unrhyw bryd. Lle y byddwch yn dewis gwneud hyn bydd angen i chi gysylltu â'r Ganolfan Byd Gwaith, yn ysgrifenedig, i ofyn iddynt ddileu eich manylion o LMS.

I gael rhagor o wybodaeth am Y Ddeddf Diogelu Data ewch i'r dudalen diogelu data yn www.dwp.gov.uk/cymraeg/privacy-policy.

DPA3: Request to Remove Client Details in LMS

To complete a Request to Remove Client Details in LMS form you must:

- Complete parts 1, 2 and 3 of the form; and
- Forward the form to your Business/Contact Centre Manager (or nominated officer of Band E or above) to complete the fields in part 4.

Part 1: Request Raised by	
Name:	
Office Name:	
Office Mnemonic:	
Telephone Number:	

Part 2: Customer Details	
Client Name:	
Client NINo:	

Part 3: Details of data to be removed	
Window Name:	
Field Name:	
Dates where appropriate:	

Part 4: Request Approved by	
Approved by (<i>Band E or above</i>):	
Telephone Number:	

| Email this form to DWP OITC Team.

NB: a request to remove data from a customer LMS record will incur a cost. You will be asked to provide a Cost Centre number *after* an initial investigation has been made into your request and deemed genuine.