Report of the Section 151 Officer

Pension Fund Committee - 5 July 2018

General Data Protection Regulations (GDPR)

Purpose:	To receive an update on The City & County of Swansea Pension Fund's action plan to comply with GDPR requirements.
Consultation:	Legal, Finance and Access to Services.
Report Author:	Jeffrey Dong
Finance Officer:	Jeffrey Dong
Legal Officer:	Stephanie Williams
Access to Services Officer:	Sherill Hopkins
For Information	

1 Background

1.1 The basic objective of the GDPR is to enforce stronger data security and privacy rules among organisations when it comes to protecting personal data. It will apply from May 25 2018. Currently, the UK relies on the Data Protection Act 1998 but this will be superseded by the new legislation.

1.2 It's important to remember that data protection requirements have been in place for many years. Although GDPR does broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the Data Protection Act 1998

2 Main Principles of GDPR

2.1 It provides important points on our responsibilities when collecting and processing personal data. We ensure :

- we have a legal basis for ***collecting*** personal data from citizens;
- the personal data we hold is ***accurate*** and up-to-date.
- we dont ***keep*** personal data longer than necessary;
- we provide a ***privacy notice*** to tell citizens what we do with their personal data;
- we insert a ***privacy statement*** on all data collection documents;
- we get ***consent*** to use the citizens personal data (where required);
- we maintain a ***record*** of all personal data processing activites;
- we assess the ***risk*** associated with the processing of personal data;
- we ***report*** a data breach;
- we ***appoint*** a Data Protection Officer.

It also identifies the rights of citizens. They have a right to:

- ***object*** to the processing of their personal data;
- ***access*** their personal data we hold - free of charge;
- request the ***deletion*** of their personal data we hold;

3 The City & County of Swansea Pension Fund

3.1 The City & County of Swansea Pension Fund is administered by Swansea Council and leverages off many of the support services of that organisation, and shares many of its control functions. The Council's Information Governance Unit has produced a fact sheet attached at Appendix 1.

3.2 Attached at Appendix 2 are the Pension Fund's :

- Full GDPR Privacy Notice
- Employer's Memorandum of Understanding
- Member FAQs

These documents have been written in consultation with the Council's Data Governance Unit as well as LGPS national guidance provided by LGA, who have taken advice from Legal Counsel.

3.3 The Pension Fund Committee is asked to note the documents in 3.2.

Background Paper: None.

Appendices: Appendix 1 - Practical Guide to GDPR
Appendix 2 Privacy Notice; Memorandum of understanding; FAQs

A practical guide to GDPR

Cyngor Abertawe
Swansea Council

25th May 2018

This is when the General Data Protection Regulation (GDPR) will come into force. If you handle personal data in your role, it is essential that you are aware of the requirements.

This guide identifies the key aspects of GDPR. It will help you to be more aware about the personal data you collect from our citizens, how you protect this data and the requirements needed to share it.

The Data Protection Act

Firstly, it is important to remember that data protection requirements have been in place for many years. Although GDPR does broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the Data Protection Act 1998.

As we already comply with existing data protection legislation, it is a good start towards compliance with GDPR as there is a degree of common ground between the two. However, in order to ensure compliance, we will need to have a thorough understanding of the new regulation.

Throughout this guide, you will see this icon (inset). It will highlight handy tips that must be taken seriously and actions put in place.

Thank you,
Information Governance Unit

INDEX

A Message from our Chief Executive

Information security is of great importance to the Council and we are committed to preserving the confidentiality, integrity, and availability of our data for sound decision-making, delivering quality services and complying with legal requirements.

Unauthorised access, loss or damage to any data we hold can cause problems for our business, customers, citizens, and third parties. We have identified failure to comply with GDPR as one of our key corporate risks and are putting in place measures that will help us achieve it.

Should compliance not be attained then the Council can risk, at worst, the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner. It you are uncertain as to the correct course of action or are suspicious about a set of circumstances, your duty is to consult your manager for advice.

Phil Roberts

Key Aspect 1 – Useful Definitions

Here are some key words (with definitions) that will be used throughout this practical guide:

Data Subjects

The data we collect and hold sometimes consists of details relating to a living individual (data subject). These are our citizens and they rely on us to keep their data safe.

Personal Data

This relates to a set of information that can identify a data subject or data subjects. As well as obvious personal identifiers in the data such as name and address, under GDPR this includes such things as genetic and biometric data.

Sensitive Personal Data

This relates to data which reveals an individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sex life.

The presumption is that, because information about these matters could be used in a discriminatory way and is likely to be of a private nature, sensitive personal data needs to be treated with greater care than other personal data.

Data Controller

This is the body which determines the purposes for which personal/sensitive data is processed. The Council as a whole is classed as a data controller so for our vast majority of our processing, Swansea Council is the named data controller.

Cyngor Abertawe
Swansea Council

Key Aspect 2 – The Six GDPR Principles

As data controller, we must be accountable and keep records evidencing our compliance with the following GDPR principles. Such record keeping would include the logging of any new system onto our Information Asset Register.

1. Lawfulness, fairness and transparency

Personal data can only be processed if there is a lawful reason for doing so. It must be fair to the data subject and you must be fully transparent with the data subject as to why you are collecting their data and how it is going to be used and shared.

2. Purpose Limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, although further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted in certain circumstances.

3. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Where personal data is inaccurate every reasonable step should be taken to enable its deletion (where appropriate) or correction without delay.

5. Storage Limitation

Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary. Such personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in certain circumstances and subject to the implementation of the appropriate technical and organisational measures.

6. Integrity and Confidentiality

Personal data must be processed in an appropriately secure manner including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

Key Aspect 3 – Rights of the Data Subject

One of the key factors of GDPR is that data subjects are granted certain rights and protections relating to their personal data. This includes:

Collecting their Data

When we collect data from our citizens, we must *inform* them about the reasons why we are collecting it and their rights. We also have a duty to ensure the data collection is *limited* to what is necessary in relation to its purpose and we don't use it for a *different* purpose without consent or seeking legal advice beforehand.

Here are the four reasons why we are able to lawfully process personal data:

1. **Legal obligation**: the processing is necessary to comply with a legal obligation. If your service is statutory, this is the basis for you;
2. **Public task**: the processing is necessary to perform a task in the public interest or in the exercise of official authority. This is where you are empowered by law but not obliged to provide a service (e.g. council housing);
3. **Contract**: the processing is necessary as part of a stated or implied contract. This will apply where you offer paid-for or free membership schemes, such as Library membership or the Active Swansea scheme;
4. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. This is the least favoured of your options because it gives increased responsibility for your data management.

So, if you collect personal data through an application form or survey for example, you must stipulate on the form "Why we are collecting this data" and "What we are going to do with the data" (privacy statement). You must also provide a link to the Council's privacy notice.

If you do not need to find out their date of birth for example when gathering the data on the form, you *must not ask for it!*

If you use this data for a different purpose without getting consent from the data subject, then you are breaking the second GDPR principle of purpose limitation.

Key Aspect 3 – Rights of the Data Subject

Objecting to use their Data

The GDPR includes the "right to object" meaning that the data subject can object to the processing of their personal data. If the objection is to direct marketing, the data subject does not need to give any reasons and staff must comply with the request.

When the data subject objects to other types of processing (i.e. not direct marketing) there are exemptions that apply. You will need to discuss this with your manager and take advice from the IGU before proceeding.

To demonstrate that you are complying with the GDPR first principle of processing personal data, that it is processed lawfully, fairly and in a transparent manner, you must maintain a record of any request made under the right to object to processing and notify the IGU of your actions.

Review existing processes to ensure that where you undertake marketing communications with citizens by email, you include an 'unsubscribe' option to allow them to object to the use of their information.

Accessing their Data

Our citizens are able to access their data via a subject access request. These requests must be handled without delay and within one month of receipt.

We must provide this information free of charge from 25th May 2018 and it is imperative that requests are taken seriously and handled efficiently.

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Key Aspect 3 – Rights of the Data Subject

Accurate Data

At all times, we must ensure that the data we have collected from our citizens now or in the past is accurate and up-to-date. Staff must take reasonable steps to ensure that where data is inaccurate, it is *rectified* without delay.

Just imagine your personal data being sent to the wrong address by your bank because the wrong house number was on their ICT system. How would you feel if your neighbour had opened the letter and read certain personal details about you?

Everyone is busy but staff are sometimes more concerned with completing their tasks than ensuring the data of our citizens is secure. This must change under GDPR or you are putting the Council at risk of fines and reputational damage.

Citizens have the right to contact the Information Commissioner to report where we have failed to keep their data accurate or their data has been breached. This could result in compensation to the citizen on top of the fine.

Storing Data

Citizens have the right to ensure that their data is not kept by us for longer than is necessary. The Council has a records retention schedule that identifies how long data should be kept.

Staff must ensure *we do not hold data* any longer than required. Remember all data that we hold is open to subject access and Freedom of Information requests.

If your role consists of processing data, you are accountable for protecting this data from unauthorised or unlawful processing and against accidental loss, destruction or damage.

Encrypting data whilst being stored (e.g. encrypted USB stick) provides effective protection against unauthorised or unlawful processing. Staff are responsible for ensuring that all ICT devices are encrypted in case the device storing the data is lost or stolen. For further information on this and email encryption, view the Data Encryption & Portable Media Policy on Staffnet.

Loss of data must be reported immediately to the Information Security Officer so the breach can be investigated: infosec@swansea.gov.uk

Key Aspect 3 – Rights of the Data Subject

Deleting Data

Under certain conditions, citizens can now request the erasure of their personal data. These are the condition, one of which must be met:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed,
- where the legal basis for processing is consent, the data subject withdraws his or her consent for us to use it, or
- the personal data has passed the retention period defined in the corporate records retention schedule.

If any of our citizens' personal data has been made public via a third party then we must take reasonable steps to inform the data processors who are processing the personal data on our behalf that the data subject has requested that they want their data deleted.

The right to be forgotten only applies where the above conditions are met and there are further exemptions where we can refuse to comply with a request:

- If it conflicts with the "right of freedom and expression"
- An overriding need to adhere to legal compliance
- Reasons of public interest in the area of public health
- Scientific, historical research or public interest archiving purposes
- If the data is required for supporting legal claims.

Further information can be found on Staffnet:

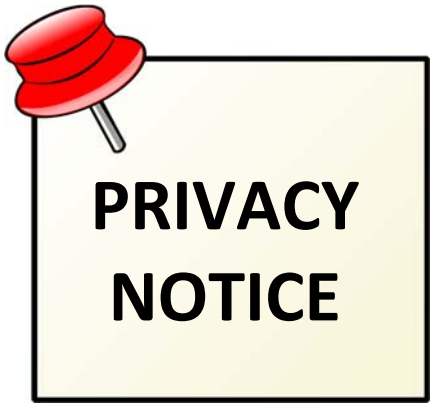
http://www.swansea.gov.uk/staffnet/RightToBeForgotten

Key Aspect 4 – Privacy Notices

Communicating with our Citizens

Being transparent and providing accessible information to our citizens about how you will use their data is a key element of the GDPR. We must inform the data subjects at the first point of contact what to expect when we collect their personal data.

As part of our journey to GDPR compliance, we have written a new bilingual corporate privacy notice, which sits on our website.



This privacy notice must be embedded as a link in your correspondence when you are asking citizens to provide their personal data e.g. on an application or service request form.

We are also working together to create a simpler privacy notice that is child friendly. We will use straightforward language and adopt a simple style (including images) that children will find easy to understand.

Once available, this too will be placed on our website.

Inserting a Privacy Statement

When collecting personal data from the public (typically this is achieved through an online or a paper form), you have to provide more specific information than is contained in the overarching corporate privacy notice.

You must ensure there is a short privacy statement on the data collection document which explains your use of the data, who you share it with and what is the legal basis for your processing the data.

For more information see:
http://www.swansea.gov.uk/staffnet/gdprprivacynotices

As mentioned in page 6 of this guide, there are four main legal reasons for the Council to be able to capture and process personal data and all data collection forms must make clear what the legal basis for processing is, if we want to be compliant with GDPR.

Key Aspect 5 – Providing Consent

Can we process this Data?

We have already mentioned that consent is one of the legal reasons for processing and if we can avoid relying on consent then we should do so. Here is why:

An indication of consent must be unambiguous and involve a clear affirmative action.

If you are collecting sensitive data, the bar is set even higher. In that case you will need explicit consent, such as a written signed statement from the data subject.

Dear Swansea Council

I did not give my consent for you to use my personal details for this!

Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Consent involves presenting the data subject with a clear statement regarding the personal data to be collected; and an explicit action agreeing with this statement (such as ticking a box saying 'I agree').

The form should say, "I consent" (or similar) for consent to be considered valid. *Silence or pre-ticked boxes* on webpages are banned under GDPR as they do not establish explicit consent.

Withdrawing Consent

The GDPR gives a specific right to withdraw consent. Where we are collecting data which is legally based on consent, we need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

We need to review our existing consents mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

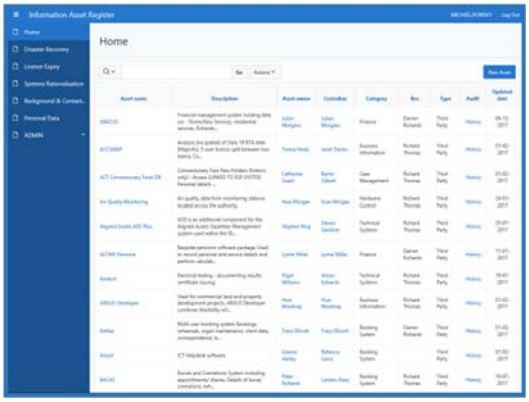
It is important for staff to maintain appropriate records in order to evidence consent has been given.

Key Aspect 6 – Register of Processing Activity (ROPA)

Maintain a Register

One of the requirements of GDPR is to maintain a record of all the processing activities that take place within the Council. For this, we need to identify:

- what personal data we process;
- what is the lawful basis for processing;
- how we store and keep the data secure;
- who has access to it;
- who we share the data with and what sharing agreements are in place;
- how long we keep it for.



The Council's RoPA is called the *Information Asset Register (IAR)*. This is held on Staffnet and identifies all the systems that hold personal data.

When updating the IAR, you must ensure you are named on there as the owner or the custodian of the asset or you will not have the permissions to add any detail and save.

http://www.swansea.gov.uk/staffnet/informationassetregister

Providing an overview

The IAR will provide an overview of all data processing activities within our Council, and therefore enable us to demonstrate to the Information Commissioner what personal data is being processed, by whom and why.

Your responsibility

If you collect and hold personal data electronically within your service then you must identify the system on the IAR. You must keep this information up-to-date.

NOTE: If you have not identified your system on the IAR and a data breach happens within your area, the ICO will hand out far more significant fines.

Key Aspect 7 – Data Protection Impact Assessments

Assessing the Risk

Data Protection Impact Assessments (DPIA) are a method that we must introduce under GDPR for *assessing the risk* associated with the processing activity we undertake of personal data.

Whenever a new system is being designed or introduced, or an existing system is being changed via a project, staff must undertake a DPIA to determine the risk to individuals' privacy associated with the processing. Further guidance will be available on Staffnet:

A DPIA will:

- Help the project have a clear data protection focus
- Allow appropriate organisational and technological measures to safeguard information to be built into any new operation.
- Challenge the designer to develop a way of working that will promote data protection principles
- Give practical solutions to enable a data subject to exercise their rights.

Just like the equalities impact assessments already undertaken within the Council, if you are not sure a full assessment is needed, you carry out a simple screening exercise which will guide your decision.

Data protection should not be a secondary function or consideration when designing a new processing activity. It is vital therefore, that staff, project leads and managers do not leave data protection principles and citizens' rights under GDPR to be considered at a late stage of the planning and design process.

Under GDPR, failure to carry out an impact assessment where one is necessary can lead to enforcement activity and a fine from the Information Commissioner.

Further information regarding DPIA can be obtained on Staffnet:
http://www.swansea.gov.uk/staffnet/dpia

Key Aspect 8 – Data Breaches

Reporting a Loss

The Council has an existing process in place to detect, report and investigate a personal data breach. The Information Governance Unit are responsible for investigating and reporting all data breaches within the Council.

However, GDPR brings in a new breach notification timeframe under which we will have to notify the Information Commissioner of serious breaches within 72 hours of discovery of the breach. A failure to report a breach within the timeframe could itself result in a fine, as well as a fine for the breach itself.

These fines can be significant sums which, with the reputational loss that comes with the associated press coverage, may impact severely on the work of the Council and the trust that our data subjects have in us to handle their personal data responsibly.

Impact of a Data Breach

The first 24 hours are critical! A data breach can potentially have a range of significant adverse effects on the rights and freedoms of data subjects. The breach may cause them physical, material or non-material damage. They may as a result of the breach be at risk of domestic violence or of credit card fraud.

The procedure for data breach reporting is identified on Staffnet: http://www.swansea.gov.uk/staffnet/databreaches

Staff must respond quickly and efficiently to lower the impact of the breach.

Key Actions

When a data breach occurs, here are the *key actions* to undertake:

- if there is a high risk to the data subject from the breach(e.g. identify theft, fraud or domestic violence), they need to be told straight away so they can take actions to protect themselves;
- Containment is key. If we can retrieve the data for the unauthorised recipient, go get it straightaway;
- When retrieving the data from them, confirm that no copies of the data has been made or shared;
- Ask if they have read the whole document or just parts and if they know the person who should have initially received this information.
- Report the breach – infosec@swansea.gov.uk

Key Aspect 9 – Data Protection Officer (DPO)

GDPR introduces a requirement to appoint or designate a Data Protection Officer (DPO) with formal responsibility for data protection compliance across the Council.

The tasks of the DPO include:

- Informing and advising its employees of their data protection obligations,
- Monitoring compliance of policies and procedures. This includes monitoring responsibilities and training of staff involved in data processing,
- Ensuring the RoPA is an active register that identifies all systems that hold personal data;
- Advising on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes,
- Serve as the contact point for all data protection issues, including managing risks and data breach reporting,
- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

WATCH OUT!

GDPR is coming and it will impact us all.

Remember, under GDPR, processing personal data without identifying and recording the lawful basis for your processing on the Information Asset register runs the risk of enforcement activity, including substantial fines, by the ICO.

Please keep our citizens' personal data secure at all times.

Information Governance Unit (IGU)

Email: Information.governance@swansea.gov.uk

Breach notification: infosec@swansea.gov.uk

Website: http://www.swansea.gov.uk/staffnet/IGU

Appendix 2

City and County of Swansea Pension Fund
Cronfa Bensiwn Dinas a Sir Abertawe

FULL PRIVACY NOTICE

for the members and beneficiaries of the City and County of Swansea Pension Fund

This notice is for members and beneficiaries of the City and County of Swansea Pension Fund (the "Fund"). It has been prepared by Swansea Council (the "Administering Authority", or "we") in its capacity as the administering authority of the Fund.

This privacy notice is also provided at the following link:

http://www.swanseapensionfund.org.uk/

Why we are providing this notice to you

As the Administering Authority of the Fund, we hold certain information about you ("personal data") which we use to administer the Fund and to pay benefits from it. This notice is designed to give you information about the data we hold about you, how we use it, your rights in relation to it and the safeguards that are in place to protect it.

What is the legal basis for our use of your personal data?

The Administering Authority holds personal data about you in its capacity as data controller for the proper handling of all matters relating to the Fund, including its administration and management. This includes the need to process your data to contact you, to calculate, secure and pay your benefits. For example, when we assess how much money is needed to provide members' benefits and how that money should be invested, and to manage liabilities and administer the Fund generally. Further information about how we use your personal data is provided below.

The legal basis for our use of your personal data will generally be one or more of the following:

a) we need to process your personal data to satisfy our legal obligations as the Administering Authority of the Fund; and
b) we need to process your personal data to carry out a task in the public interest or in the exercise of official authority in our capacity as a public body; and
c) we need to process your personal data for the legitimate interests of administering and managing the Fund and liabilities under it, calculating, securing and paying benefits and performing our obligations and exercising any rights, duties and discretions the Administering Authority has in relation to the Fund; and
d) because we need to process your personal data to meet our contractual obligations to you in relation to the Fund (for example, under an agreement that

you will pay additional voluntary contributions to the Fund), or to take steps, at your request, before entering into a contract.

What personal data do we hold, and how do we obtain it?

The types of personal data we hold and process about you can include:

- Contact details, including name, address, telephone numbers and email address.
- Identifying details, including date of birth, national insurance number and employee and membership numbers*.*
- Information that is used to calculate and assess eligibility for benefits, for example, length of service or membership and salary information.
- Financial information relevant to the calculation or payment of benefits, for example, bank account and tax details.
- Information about your family, dependents or personal circumstances, for example, marital status and information relevant to the distribution and allocation of benefits payable on death.
- Information about your health, for example, to assess eligibility for benefits payable on ill health, or where your health is relevant to a claim for benefits following the death of a member of the Fund.
- Information about a criminal conviction if this has resulted in you owing money to your employer or the Fund and the employer or Fund may be reimbursed from your benefits.

We obtain some of this personal data directly from you. We may also obtain data (for example, salary information) from your current or past employer(s) or companies that succeeded them in business, from a member of the Fund (where you are or could be a beneficiary of the Fund as a consequence of that person's membership of the Fund) and from a variety of other sources including public databases (such as the Register of Births, Deaths and Marriages), our advisers and government or regulatory bodies, including those in the list of organisations that we may share your personal data with set out below.

Where we obtain information concerning certain "special categories" of particularly sensitive data, such as health information, extra protections apply under the data protection legislation. We will only process your personal data falling within one of the special categories with your consent, unless we can lawfully process this data for another reason permitted by that legislation. You have the right to withdraw your consent to the processing at any time by notifying the Administering Authority in writing. However, if you do not give consent, or subsequently withdraw it, the Administering Authority may not be able to process the relevant information to make decisions based on it, including decisions regarding the payment of your benefits.

Where you have provided us with personal data about other individuals, such as family members, dependants or potential beneficiaries under the Fund, please ensure that those individuals are aware of the information contained within this notice.

How will we use your personal data?

We will use this data to deal with all matters relating to the Fund, including its administration and management. This can include the processing of your personal data for all or any of the following purposes:

- to contact you.
- to assess eligibility for, calculate and provide you (and, if you are a member of the Fund, your beneficiaries upon your death) with benefits.
- to identify your potential or actual benefit options.
- to allow alternative ways of delivering your benefits, for example, through the use of insurance products and transfers to or mergers with other pension arrangements.
- for statistical and financial modelling and reference purposes (for example, when we assess how much money is needed to provide members' benefits and how that money should be invested).
- to comply with our legal and regulatory obligations as the administering authority of the Fund.
- to address queries from members and other beneficiaries and to respond to any actual or potential disputes concerning the Fund.
- the management of the Fund's liabilities, including the entering into of insurance arrangements and selection of Fund investments.
- in connection with the sale, merger or corporate reorganisation of or transfer of a business by the employers that participate in the Fund and their group companies.

Organisations that we may share your personal data with

From time to time, we will share your personal data with advisers and service providers so that they can help us carry out our duties, rights and discretions in relation to the Fund. Some of those organisations will simply process your personal data on our behalf and in accordance with our instructions. Other organisations will be responsible to you directly for their use of personal data that we share with them. They are referred to as data controllers and we have highlighted them in the table below. You will be able to find out about their own data protection policies (which will apply to their use of your data) on their websites. A brief description from our actuarial services/benefits/governance provider, Aon Hewitt Limited on how they use your personal data in order to support us in the running of the Scheme, is provided in Appendix 1 attached to this notice.

These organisations include the Fund's:

Data processors	**Data controllers**
• Administrator – currently Swansea Council • Third party administrators – JLT Limited • Accountants – currently Swansea Council • Tracing bureaus for mortality screening and locating members – currently ATMOS Data Services/Swansea Council • Overseas payments provider to transmit payments to scheme member with non-UK accounts – currently Western Union • Printing companies – currently Adare and DesignPrint • Pensions software provider – currently Aquila Heywood • Suppliers of IT, document production and distribution services – currently Aquila Heywood	• Actuarial consultant – currently AON Hewitt • Scheme benefit consultant – currently AON Hewitt • Investment adviser – currently Swansea Council • Additional Voluntary Contribution providers – currently Equitable Life, Prudential, AEGON • Legal adviser – currently Swansea Council • Fund Actuary – currently AON Hewitt • Statutory auditor – currently Wales Audit Office • External auditor – currently Wales Audit Office • Internal auditor – currently Swansea Council • Insurance companies in connection with ill health benefits – (N/A) • LGPS National Insurance database – (South Yorkshire Pensions Authority) • The Department for Work and Pensions • The Government Actuary's Department • The Cabinet Office – for the purposes of the National Fraud Initiative • HMRC • The Courts of England and Wales – for the purpose of processing pension sharing orders on divorce

In each case, we will only do this to the extent that we consider the information is reasonably required for these purposes.

In addition, where we make Fund investments or seek to provide benefits for Fund members in other ways, such as through the use of insurance, then we may need to

share personal data with providers of investments, insurers and other pension scheme operators. In each case, we will only do this to the extent that we consider the information is reasonably required for these purposes.

From time to time we may provide some of your data to your employer and their relevant subsidiaries (and potential purchasers of their businesses) and advisers for the purpose of enabling your employer to understand its liabilities to the Scheme. Your employer would generally be a controller of the personal data shared with it in those circumstances. For example, where your employment is engaged in providing services subject to an outsourcing arrangement, the Administering Authority may provide information about your pension benefits to your employer and to potential bidders for that contract when it ends or is renewed.

Where requested or if we consider that it is reasonably required, we may also provide your data to government bodies and dispute resolution and law enforcement organisations, including those listed above, the Pensions Regulator, the Pensions Ombudsman and Her Majesty's Revenue and Customs (HMRC). They may then use the data to carry out their legal functions.

The organisations referred to in the paragraphs above may use the personal data to perform their functions in relation to the Fund as well as for statistical and financial modelling (such as calculating expected average benefit costs and mortality rates) and planning, business administration and regulatory purposes. They may also pass the data to other third parties (for example, insurers may pass personal data to other insurance companies for the purpose of obtaining reinsurance), to the extent they consider the information is reasonably required for a legitimate purpose.

In some cases, these recipients may be outside the UK. This means your personal data may be transferred outside the EEA to a jurisdiction that may not offer an equivalent level of protection as is required by EEA countries. If this occurs, we are obliged to verify that appropriate safeguards are implemented with a view to protecting your data in accordance with applicable laws. Please use the contact details below if you want more information about the safeguards that are currently in place.

We do not use your personal data for marketing purposes and will not share this data with anyone for the purpose of marketing to you or any beneficiary.

How long will we keep your personal data?

We will only keep your personal data for as long as we need to in order to fulfil the purpose(s) for which it was collected and for so long afterwards as we consider may be required to deal with any questions or complaints that we may receive about our administration of the Fund; unless we elect to retain your data for a longer period to comply with our legal and regulatory obligations. In practice, this means that your personal data will be retained for such a period as you (or any beneficiary who receives benefits after your death) are entitled to benefits from the Fund. For the same reason, your personal data may also need to be retained where you have received a transfer, or refund, from the Fund in respect of your benefit entitlement. We will need to retain

personal data held for the purposes of the Fund for extended periods because of the long-term nature of the pension liabilities.

Your rights

You have a right to access and obtain a copy of the personal data that the Administering Authority holds about you, and to ask the Administering Authority to correct your personal data if there are any errors or it is out of date. In some circumstances you may also have a right to ask us to restrict the processing of your personal data until any errors are corrected, to object to processing or to transfer or (in very limited circumstances) erase your personal data. You can obtain further information about these rights from the Information Commissioner's Office at: www.ico.org.uk or via their telephone helpline (0303 123 1113).

If you wish to exercise any of these rights or have any queries or concerns regarding the processing of your personal data, please contact the Fund Administrator below. You also have the right to lodge a complaint in relation to this privacy notice, or the Administering Authority processing activities with the Information Commissioner's Office, which you can do through the website above or their telephone helpline.

The personal data we hold about you is used to administer your Fund benefits and we may from time to time ask for further information from you for this purpose. If you do not provide such information, or ask that, the personal data we already hold is deleted or restricted this may affect the payment of benefits to you (or your beneficiaries) under the Fund. In some cases, it could mean the Administering Authority is unable to put your pension into payment or has to stop your pension (if already in payment).

Updates

We may update this notice periodically. Where we do this, we will inform members of the changes and the date on which the changes take effect.

Contacting us

Please contact the Fund Administrator City and County of Swansea Pension Fund for further information.

Telephone number: 01792 636655
Email: pensions@swansea.gov.uk
Postal Address:
Pension Section
Swansea Council
Civic Centre
Oystermouth Road
SWANSEA
SA1 3SN

Data Protection Officer

You may also contact our data protection officer for further information: data.protection@swansea.gov.uk

Appendix 1

AON HEWITT LIMITED "QUICK READ" PRIVACY NOTICE

Aon Hewitt Limited ("Aon") has been appointed to provide pensions advisory and calculation services that relate to your membership of the Fund. In doing so Aon will use personal information about you, such as your name and contact details, information about your pension contributions, age of retirement, and in some limited circumstances information about your health (where this impacts your retirement age) in order to be able to provide these services. The purposes for which we use personal information will include management of the Fund and your membership within it, funding (i.e. helping to ensure that the funds held within the Fund are sufficient to cover the members who are party to it), liability management (that is to say providing advice on the different ways benefits could be determined, and drawn, from the Fund), Fund Actuary duties (which include assessing individuals who are members of the pension scheme and assessing how the make-up of the membership may affect the amounts payable and when they become payable so as to manage the Fund appropriately), regulatory compliance, process and service improvement and benchmarking.

We may pass your personal information to third parties such as financial advisors and benefits providers, insurers, our affiliates and service providers and to certain regulatory bodies where legally required to do so. Depending on the circumstances, this may involve a transfer of data outside the UK and the European Economic Area to countries that have less robust data protection laws. Any such transfer will be made with appropriate safeguards in place.

More detail about Aon's use of your personal information is set out in our full Privacy Notice. We recommend that you review this notice which is available online at http://www.aon.com/unitedkingdom/products-and-services/human-capital-consulting/aon-hewitt-actuarial-services-privacy-statement.jsp, or you can request a copy by contacting us, including reference to the Fund name, at: Data Protection Officer, Aon Hewitt Limited (Retirement and Investment UK), PO Box 730, Redhill, RH1 9FH

Date of issue: April 2018

City and County of Swansea Pension Fund
Cronfa Bensiwn Dinas a Sir Abertawe

LOCAL GOVERNMENT PENSION SCHEME

Memorandum of Understanding regarding Compliance with Data Protection Law

1 INTRODUCTION

1.1 The Local Government Pension Scheme ("**LGPS**") in England and Wales is an occupational pension scheme registered under section 153 of the Finance Act 2004 and its rules are currently set out in The Local Government Pension Scheme Regulations 2013 (SI 2013/2356) as amended ("**LGPS Regulations**").

1.2 The LGPS is administered locally by administering authorities which are defined in Regulation 2 of the LGPS Regulations and listed in Part 1 of Schedule 3 of the LGPS Regulations.

1.3 Swansea Council ("**Administering Authority**") is an administering authority under the LGPS Regulations. The Administering Authority manages and administers the City and County of Swansea pension fund within the LGPS (the "**Fund**") in accordance with its statutory duty under Regulation 53 of the LGPS Regulations. Employers employing employees who are eligible to be members of the LGPS will participate in the Fund as a "**Scheme Employer**" (as defined in schedule 1 of the LGPS Regulations). The Administering Authority and the Scheme Employer (together the "**Parties**") are required to share personal data relating to the Scheme Employer's current and former employees who participate in the Fund (the "**Members**") and their dependants, in order for the Administering Authority to fulfil its statutory duties to manage and administer the Fund under Regulation 53 of the LGPS Regulations and provide the Members with benefits upon retirement, pay ill-health benefits, pay death grants, pay survivors' pensions to Members' spouses, civil partners and co-habiting partners, pay children's pensions upon the death of the Member, offer Members the option of paying additional voluntary contributions to one or more providers in accordance with Regulations 1 – 52 of the LGPS Regulations.

1.4 Scheme Employers are under a statutory obligation, as detailed in Regulation 80 of the LGPS Regulations, to provide certain personal data relating to its Members on an annual basis to the Administering Authority, including the Member's name, gender, date of birth, national insurance number, pensionable pay, employer and employee pension contributions, details of any additional pension contributions and additional voluntary contributions. The City and County of Swansea Pension Fund requires this information to be provided on a monthly basis by the Employer, the timeliness and quality of which is monitored in accordance with the Pension Administration Strategy.

1.5 This Memorandum of Understanding sets out:

(a) the basis on which data will be shared between the Parties;

(b) the Administering Authority's expectations of the Scheme Employer during its participation in the Fund;

in order to comply with Data Protection Law, including the General Data Protection Regulation (2016/679) ("**GDPR**") which will have direct legal effect in the UK on and after 25 May 2018.

1.6 References to "**Data Protection Law**" in this Memorandum of Understanding mean the Data Protection Act 1998, the Data Protection Directive (95/46/EC), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended), the General Data Protection Regulation (2016/679) and all applicable laws and regulations relating to personal data and privacy which are enacted from time to time, including (where applicable) the guidance and codes of practice issued by the Information Commissioner's Office and any other competent authority.

2 DATA CONTROLLERS

2.1 The Parties acknowledge that they will:

(a) not hold a pool of joint data to which both parties have access;

(b) be separate and independent data controllers in relation to the copies of the Members' personal data they respectively hold;

(c) act as data controller in relation to personal data transferred to them;

(d) each be responsible for complying with the requirements in Data Protection Law that are applicable to them as data controllers.

Please refer to the City and County of Swansea Pension Fund Privacy Notice for further information concerning who we share data with.

2.2 References to Members' personal data includes personal data relating to the Members' dependants (including children) and spouses/civil partners (where applicable).

3 DATA SHARING

3.1 The Parties confirm that they understand their respective obligations under Data Protection Law as data controllers and agree to only process personal data relating to the Members:

(a) fairly and lawfully and in accordance with the data protection principles set out in Data Protection Law;

(b) where there are lawful grounds for doing so; and

(c) in accordance with Data Protection Law and best practice guidance (including the Data Sharing Code issued by the Information Commissioner's Office and updated from time to time).

3.2 Each Party will separately inform the Members (as required under Data Protection Law) of the respective purposes for which they will each process their personal data and provide all required information to ensure that the Members understand how their personal data will be processed in each case by the Administering Authority or Scheme Employer (as applicable). The Scheme Employer's privacy notice to Members will inform them that their personal data will be provided to the City and County Pension Fund.

3.3 Each Party confirms that it understands its respective obligations under Data Protection Law, to ensure that the Members' personal data of which it is a data controller is kept and used securely at all times and to take such technical and organisational security measures against unauthorised and unlawful processing of, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Members' personal data transmitted, stored or otherwise processed as may be required. Such measures will have due regard to the state of technological development and the cost of implementation of these measures, to ensure a level of security appropriate to the harm that might result from such processing and the nature, scope, context and purposes of processing the Members' personal data and the risk or likelihood and severity for the rights and freedoms of data subjects. Such measures will ensure:

(a) the ongoing confidentiality, integrity, availability and resilience of processing the Members' personal data;

(b) the ability to restore the availability and access to the Members' personal data in a timely manner in the event of a physical or technical incident;

(c) carrying out of regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.4 Each Party undertakes to notify the other as soon as practicable if an error is discovered in the Members' personal data of which it is a data controller and which was received from or a copy of which has been provided to the other Party, to ensure that such other Party is then able to correct its own records. This will happen whether the error is discovered through existing data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Administering Authority or Scheme Employer (as appropriate) by the Member (or the Member's dependants, spouse/civil partner) themselves).

4 TRANSFER OF MEMBERS' PERSONAL DATA

4.1 The Parties agree that Members' personal data will only be transferred from one Party to the other via an acceptable method specified by the Administering Authority which may include any of the following:

(a) face to face

(b) courier

(c) secure email

(d) SFTP link

(e) encrypted removable media

(f) access secure website

(g) third party solution as agreed by the Parties

4.2 Each Party will, when transferring the Members' personal data of which it is the data controller to the other Party, ensure that that data is secure during transit (whether physical or electronic).

4.3 If either the Administering Authority or the Scheme Employer appoints professional advisers, third party administrators or another entity which provides other services involving the transfer of Members' personal data, those third parties will be data processors or data controllers in their own right. The Administering Authority or the Scheme Employer (as applicable) will comply with its own obligations in accordance with Data Protection Law (in particular, by ensuring that any entity to which it transfers Members' personal data also complies with Data Protection Law) and shall ensure that that nothing in the terms of engagement between the Administering Authority or the Scheme Employer (as applicable) and such third party would contradict this Memorandum of Understanding.

5 RIGHTS OF MEMBERS (INCLUDING THE MEMBER'S DEPENDANTS, SPOUSES/CIVIL PARTNERS (WHERE APPLICABLE))

5.1 Each Party shall, in respect of the personal data of which it is a data controller, respond to any requests from Members to have access to any of their personal data or a complaint or enquiry relating to that Party's processing of the Members' personal data received by that Party in line with its own obligations under the Data Protection Law.

5.2 Each Party agrees to provide reasonable assistance to the other as is necessary to enable the other Party to comply with any such requests in respect of Members' personal data of which that Party is a data controller and to respond to any other queries or complaints from Members.

6 DATA SECURITY BREACHES AND REPORTING PROCEDURES

6.1 Each Party has in place a formal process for reporting breaches under Data Protection Law. Where a significant data breach occurs (significant in the opinion of the individual party in consideration of the obligations imposed by the Data Protection Law) it will inform the other party of the breach where it is believed such action will improve/mitigate any impact to the member and where necessary notify the Information Commissioner's Office and/or the Member(s).

7 RESPONSIBILITIES OF SCHEME EMPLOYERS

7.1 Notwithstanding the statutory obligations which apply to Scheme Employers under the LGPS Regulations and as a data controller under Data Protection Law, the Administering Authority, as Administering Authority for the Fund, expects Scheme Employers participating in the Fund to comply with the responsibilities set out below in relation to Members' personal data.

7.2 On request, the Scheme Employer will inform the Funds Data Protection Officer; data.protection@swansea.gov.uk at the Administering Authority or any appointed qualified person to fulfil the role of Data Protection Officer together with their contact details. If the Scheme Employer has not appointed a Data Protection Officer, the Scheme Employer on request will inform the Funds Data Protection Officer of the details of a nominated person for GDPR compliance purpose.

7.3 The Scheme Employer will demonstrate to the Administering Authority's satisfaction when dealing with ill health early retirement applications for current employees that explicit Member consent has been received which gives consent to processing by both the Scheme Employer and the Administering Authority. In the absence of such consent, the Administering Authority may not be able to process the Member's application.

7.4 The Scheme Employer acknowledges the financial penalties that can be imposed by the Information Commissioner's Office in relation to breaches of Data Protection Law [and will inform the Administering Authority immediately from the point that it becomes aware that the Scheme Employer may be liable to pay such a financial penalty]. [The Scheme Employer further acknowledges that any liability it may have to pay a financial penalty to the Information Commissioner's Office may result in a revision of the rates and adjustments certificate in accordance with Regulation 62(7) of the LGPS Regulations.]

8 COMPLIANCE WITH THE MEMORANDUM OF UNDERSTANDING

8.1 Failure by the Scheme Employer to comply with the terms set out in this Memorandum of Understanding may result in the Administering Authority taking any or all of the following actions:

(a) reporting the Scheme Employer's non-compliance to the Information Commissioner's Office;

(b) Any other action which the Administering Authority deems appropriate and which is within its powers to do so

9 REVIEW AND AMENDMENT OF MEMORANDUM OF UNDERSTANDING

The Administering Authority will review the Memorandum of Understanding periodically. The Administering Authority reserves the right to amend the Memorandum of Understanding at any time and with immediate effect and will provide written notice to the Scheme Employer of such amendment.

10. This Memorandum of Understanding will be published on the Funds website www.swanseapensionfund.org.uk with the Privacy Notice.

Signed	
Name	
Position	
Date	

Q&A for LGPS members - What is the GDPR?

The General Data Protection Regulation (GDPR) is a new set of European Union (EU) regulations due to come into force on 25 May 2018. It will change how organisations process and handle data, with the key aim of giving greater protection and rights to individuals.

What laws currently govern data protection in the UK?

Currently in the UK the Data Protection Act 1998 sets out how your personal information can be used by companies, government and other organisations. The GDPR will replace the Data Protection Act 1998 when it comes into force on 25 May 2018.

Will the GDPR still apply to the UK after Brexit?

The UK is in the process of implementing a new Data Protection Bill which largely includes all the provisions of the GDPR. There are some small differences, but once the Bill has passed through Parliament and become an Act, UK law on data protection will largely be the same as that of the GDPR.

So what's new?

There are new and extended rights for individuals in relation to the personal data an organisation holds about them, for example, an extended right to access and a new right of data portability. You can obtain further information about these rights from the Information Commissioner's Office at: www.ico.org.uk or via their telephone helpline (0303 123 1113).

In addition, organisations will have an obligation for better data management and a new regime of fines will be introduced for use when an organisation is found to be in breach of the GDPR.

What are the main principals of the GDPR?

The GDPR states that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- held only for the absolute time necessary and no longer
- processed in a manner that ensures appropriate security of the personal data.

What is personal data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, r
in technology and the way organisations collect information about peopl

How will the GDPR affect LGPS members?

Your LGPS fund will already have procedures in place which comply with similar data protection principles under the Data Protection Act 1998. The new regulations will reinforce these existing requirements, and LGPS members are unlikely to notice a change in the service they receive from their LGPS fund.

How will members know that their LGPS fund is GDPR compliant?

Every LGPS fund will be required to update their privacy notice in line with the new requirements setting out, among other things, why certain data is held, the reason for processing the data, who they share the data with and the period for which the data will be retained. Within the notice, members will also be provided with additional information about their rights under the legislation.

Why do LGPS funds hold personal data?

LGPS funds require various pieces of personal data provided by both the individual member and their employer in order to administer the pension scheme. This data includes, but is not limited to, names, addresses, National Insurance numbers and salary details which are required to maintain scheme records and calculate member benefits.

Who do LGPS funds share personal data with?

On occasion, LGPS funds are required to share personal data with third parties in order to meet regulatory and government requirements, to gather necessary information for the accurate payment of member benefits and to ensure scheme liabilities are met. Each fund's privacy notice will set out who they share data with; this is likely to include bodies such as scheme employers, fund actuaries, auditors and HMRC.

Can LGPS members ask for their data to be deleted?

The GDPR provides individuals with the 'right to be forgotten' in certain limited circumstances. However, in practical terms the exercise of this right in relation to LGPS funds is limited as the deletion of data can prevent the fund from carrying out its duties. LGPS funds are required to process personal data to comply with legal obligations under pension legislation, therefore, the 'right to be forgotten' is unlikely to apply to data held by LGPS funds.

What happens if there is a data breach?

Data breaches are a rare occurrence within LGPS funds. However, should a security breach concerning a member's personal data occur that is likely to result in a risk to that member's rights and freedoms, there will be a direct obligation under the GDPR for the fund to inform the Information Commissioners Office within 72 hours of the breach taking place.

Cyngor Abertawe
Swansea Council

Mae'r Rheoliadau Gwarchod Data Cyffredinol (GDPR) yn set newydd o reoliadau'r Undeb Ewropeaidd (UE) sydd i ddod i rym ar 25 Mai 2018. Bydd yn newid sut mae sefydliadau'n prosesu a thrin data, gyda'r nod allweddol o roi mwy o ddiogelwch a hawliau i unigolion.

Pa ddeddfau sy'n rheoli diogelu data yn y DU ar hyn o bryd?

Ar hyn o bryd yn y DU mae Deddf Diogelu Data 1998 yn nodi sut y gall cwmnïau, llywodraeth a sefydliadau eraill ddefnyddio'ch gwybodaeth bersonol. Bydd y GDPR yn disodli Deddf Diogelu Data 1998 pan ddaw i rym ar 25 Mai 2018.

A fydd y GDPR yn dal i fod yn berthnasol i'r DU ar ôl Brexit?

Mae'r DU yn y broses o weithredu Mesur Diogelu Data newydd sydd, yn bennaf, yn cynnwys holl ddarpariaethau'r GDPR. Mae yna rai gwahaniaethau bach, ond unwaith y bydd y Mesur wedi pasio drwy'r Senedd ac yn dod yn Ddeddf, bydd cyfraith y DU ar ddiogelu data yn debyg iawn i rheoliadau'r GDPR.

Felly beth sy'n newydd?

Mae hawliau newydd ac estynedig ar gyfer unigolion mewn perthynas â'r data personol y mae sefydliad yn ei chadw amdanynt, er enghraifft, hawl estynedig i gael mynediad i ddata a hawl newydd o ran symudadwyedd data. Gallwch gael rhagor o wybodaeth am yr hawliau hyn gan Swyddfa'r Comisiynydd Gwybodaeth: www.ico.org.uk neu drwy eu llinell gymorth ffôn (0303 123 1113).

Yn ogystal, bydd gan sefydliadau rwymedigaeth ar gyfer rheoli data yn well a chyflwynir cyfundrefn ddirwyon newydd i'w ddefnyddio pan ddarganfyddir bod sefydliad yn torri'r GDPR.

Beth yw prif egwyddorion y GDPR?

Mae'r GDPR yn nodi bod rhaid i ddata personol fod:

- wedi'i brosesu yn gyfreithlon, yn deg ac mewn modd tryloyw
- wedi ei gasglu at ddibenion penodol, eglur a dilys yn unig
- yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol
- yn gywir ac yn gyfoes
- wedi ei gadw am yr amser absoliwt sy'n angenrheidiol a dim mwyach
- wedi'i brosesu mewn modd sy'n sicrhau diogelwch priodol y data personol.

Beth yw data personol?

Mae'r GDPR yn berthnasol i 'ddata personol' sy'n golygu unrhyw w ymwneud â pherson adnabyddadwy y gellir ei adnabod ynunion anuniongyrchol yn benodol trwy gyfeirio at dynodwr.

Mae'r diffiniad hwn yn darparu ar gyfer ystod eang o ddynodwyr personol i gyfansoddi data personol, gan gynnwys enw, rhif adnabod, data lleoliad neu ddynodwr ar-lein, sy'n

adlewyrchu newidiadau mewn technoleg a'r modd y mae sefydliadau'n casglu gwybodaeth am bobl.

Sut fydd GDPR yn effeithio ar aelodau'r CPLlL?

Bydd gan eich cronfa CPLlL eisoes weithdrefnau yn eu lle sy'n cydymffurfio ag egwyddorion diogelu data tebyg o dan Ddeddf Diogelu Data 1998. Bydd y rheoliadau newydd yn atgyfnerthu'r gofynion presennol hyn, ac mae'n annhebygol y bydd aelodau'r CPLlL yn sylwi ar newid yn y gwasanaeth a dderbynnir gan eu cronfa CPLlL.

Sut y bydd aelodau'n gwybod bod eu cronfa CPLlL yn cydymffurfio â GDPR? Bydd gofyn i bob cronfa CPLlL ddiweddaru eu rhybudd preifatrwydd yn unol â'r gofynion newydd sy'n nodi, ymhlith pethau eraill, pam bod data penodol yn cael ei gadw, y rheswm dros brosesu'r data, pwy maent yn rhannu'r data gyda a'r cyfnod y mae'r data yn cael ei gadw. O fewn yr hysbysiad, bydd aelodau hefyd yn cael gwybodaeth ychwanegol am eu hawliau o dan y ddeddfwriaeth.

Pam mae cronfeydd CPLlL yn dal data personol?

Mae cronfeydd CPLlL angen wahanol ddarnau o ddata personol a ddarperir gan yr aelod unigol a'u cyflogwr er mwyn gweinyddu'r cynllun pensiwn. Mae'r data hwn yn cynnwys, ond heb eu cyfyngu i, enwau, cyfeiriadau, rhifau Yswiriant Gwladol a manylion cyflog, sydd eu hangen i gynnal cofnodion y cynllun a chyfrifo buddion aelodau.

Pwy y mae cronfeydd CPLlL yn rhannu data personol â nhw?

Ar adegau, mae'n ofynnol i gronfeydd CPLlL rannu data personol gyda thrydydd parti er mwyn cwrdd â gofynion rheoliadol a llywodraethol, i gasglu'r wybodaeth angenrheidiol ar gyfer talu buddion aelodau'n fanwl gywir a sicrhau bod rhwymedigaethau'r cynllun yn cael eu bodloni. Bydd rhybudd preifatrwydd pob cronfa yn nodi pwy y maent yn rhannu data â nhw; mae'n debygol y bydd hyn yn cynnwys cyrff megis cyflogwyr y cynllun, actiwarïaid y gronfa, archwilwyr a Cyllid a Thollau EM.

A all aelodau CPLlL ofyn am gael dileu eu data?

Mae'r GDPR yn darparu'r 'hawl i gael ei anghofio' mewn rhai amgylchiadau cyfyngedig. Fodd bynnag, mewn termau ymarferol, cyfyng yw arfer yr hawl hwn mewn perthynas â chronfeydd CPLlL gan y gall dileu data atal y gronfa rhag cyflawni ei ddyletswyddau. Mae'n ofynnol i gronfeydd CPLlL brosesu data personol i gydymffurfio â rhwymedigaethau cyfreithiol dan ddeddfwriaeth pensiwn, felly, mae'n annhebygol y bydd yr 'hawl i gael ei anghofio' yn berthnasol i ddata a gedwir gan gronfeydd CPLlL

Beth sy'n digwydd os oes toriad data?

Mae achosion o dorri data yn ddigwyddiad prin o fewn cronfeydd CPLlL. Fodd bynnag, pe bai toriad diogelwch yn ymwneud â data personol aelod yn digwydd sy'n debygol o arwain at berygl i hawliau a rhyddid yr aelod hwnnw, bydd rhwymedigaeth uniongyrchol o dan y GDPR ar gyfer y gronfa i hysbysu'r Swyddfa Comisiynwyr Gwybodaeth o fewn 72 awr i'r toriad yn digwydd.