Cyngor Abertawe
Swansea Council

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.

lgps 2014

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

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.

Cwestiynau ac Ate bar gyfer aelodau'r CPLIL

Beth yw'r GDPR?

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 wybodaeth sy'n ymwneud â pherson adnabyddadwy y gellir ei adnabod ynuniongyrchol neu'n 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 CPLIL?

Bydd gan eich cronfa CPLIL 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 CPLIL yn sylwi ar newid yn y gwasanaeth a dderbynnir gan eu cronfa CPLIL.

Sut y bydd aelodau'n gwybod bod eu cronfa CPLIL yn cydymffurfio â GDPR?

Bydd gofyn i bob cronfa CPLIL 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 CPLIL yn dal data personol?

Mae cronfeydd CPLIL 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 CPLIL yn rhannu data personol â nhw?

Ar adegau, mae'n ofynnol i gronfeydd CPLIL 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, actiwarïi'r gronfa, archwilwyr a Cyllid a Thollau EM.

A all aelodau CPLIL 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 CPLIL gan y gall dileu data atal y gronfa rhag cyflawni ei ddyletswyddau. Mae'n ofynnol i gronfeydd CPLIL 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.