Comisiynydd Cenedlaethau'r Dyfodol Cymru | Future Generations Commissioner for Wales

Polisi Defnydd Diawdurdod o Ddata Personol

Datganiad Polisi

Mae'r Comisiynydd wedi ymrwymo i sicrhau bod pob gwybodaeth bersonol a chorfforaethol yn cael ei chadw mewn dull priodol yn unol â gofynion y Ddeddf Diogelu Data (DPA), y Rheoliad Cyffredinol ar Ddiogelu Data (GDPR), y Ddeddf Rhyddid Gwybodaeth (FOIA) a'r Rheoliadau Gwybodaeth Amgylcheddol (EIR).

Mae'r Comisiynydd yn disgwyl i'r holl staff a chydweithwyr gydymffurfio â gofynion y polisi hwn ac i godi unrhyw faterion yn ddiymdroi fel y gall risgiau i ddata personol yr ydym yn ei gadw gael ei leihau.

Rolau a Chyfrifoldebau

- Cyfarwyddwr Cyllid a Llywodraethu Corfforaethol
- Pennaeth Adnoddau Dynol
- Swyddog Diogelu Data
- Swyddog Cyllid a Llywodraethu Corfforaethol
- Rheolwr Swyddfa

Polisi Defnydd Diawdurdod o Ddata Personol

Mae'r Rheoliad Cyffredinol ar Ddiogelu Data (GDPR) yn ei gwneud yn ofynnol i ni gael y polisi hwn yn ei le.

Beth yw Defnydd Diawdurdod o Ddata Personol?

Yn fras, gellir diffinio defnydd diawdurdod o ddata personol fel digwyddiad diogelwch sy'n effeithio ar gyfrinachedd, cywirdeb neu argaeledd data personol.

Mae GDPR yn ehangu'r diffiniad o ddefnydd diawdurdod o ddata i gynnwys:

- Mynediad gan drydydd parti heb ei awdurdodi
- Gweithredu bwriadol neu ddamweiniol (neu ddiffyg gweithredu) gan reolydd* neu brosesydd
- Anfon data personol i dderbynnydd anghywir
- Dyfeisiadau'n cynnwys data personol yn cael eu colli neu eu dwyn
- Newid data personol heb ganiatâd
- Colli argaeledd data personol

Comisiynydd Cenedlaethau'r Dyfodol Cymru | Future Generations Commissioner for Wales

Gallai defnydd diawdurdod o ddata neu golli data hefyd effeithio ar ein gallu i gyflawni ein cyfrifoldebau o dan FOIA gan y gallai gwybodaeth sy'n amodol ar FOI fod yn wybodaeth sydd heb fod ar gael.

*Mae gan y rhai sy'n rheoli data ar y cyd, gyd-rwymedigaeth petai defnydd diawdurdod yn digwydd.

Dyletswydd i hysbysu Swyddfa'r Comisiynydd Gwybodaeth

Mewn rhai amgylchiadau mae'n ofynnol i ni adrodd defnydd diawdurod/colled i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr a rhoi gwybod i wrthrych y data heb oedi (petai yna bosibilrwydd y gallai defnydd diawdurdod effeithio ar hawliau a rhyddid gwrthrych y data). Rhaid i hyn gael ei asesu ar sail un achos ar y tro a rhaid gwneud cofnod o unrhyw benderfyniad **i beidio hysbysu.**

Adrodd a Chraffu – Disgwylir i'r holl staff a chydweithwyr dynnu sylw at unrhyw bryderon neu faterion gyda'r DPO neu Reolydd Swyddfa ar unwaith; efallai y byddwn yn medru lleihau risg o ddefnydd diawdurod neu golled.

Bydd digwyddiadau colli data, neu ddata a fu bron â chael ei golli, yn cael eu hadrodd yn gyson drwy uwch dîm staff y Comisiynydd i'r Comisiynydd a'i Phwyllgor Archwilio.

Cosbau a Dirwyon – Mae GDPR yn caniatáu i'r ICO weithredu cosbau ariannol sylweddol mewn perthynas â defnydd diawdurdod o ddata/colli data. Mae hyn yn cynnwys methu cael polisi yn ei le, methu rhoi gwybod i ICO neu wrthrych data am ddefnydd diawdurdod (os yn briodol).

Mesurau Technegol a Sefydliadol

Mae GDPR yn ei gwneud yn ofynnol i ni weithredu mesurau technolegol a sefydliadol i sicrhau bod data personol yn cael ei gadw'n ddiogel a'i brosesu yn unol â hawliau gwrthrychau data. Rydyn ni'n gweithio gyda chyflenwr TG allanol (Orbits IT ar hyn o bryd) sy'n darparu caledwedd, gwasanaethau seiliedig ar rwydwaith a chwmwl i gynorthwyo arferion gwaith.

Mae'r mesurau canlynol yn eu lle i sicrhau bod ein data'n cael ei ddiogelu rhag bygythiadau allanol:

1. Mae'n ofynnol i bob dyfais sydd o dan reolaeth Orbits IT gael cyfrineiriau unigryw, cryf sy'n cael eu newid yn rheolaidd.

2. Mae systemau'n cael eu diweddaru a'u newid yn gyson pan fydd diweddariadau ar gael oddi wrth y gwneuthurwyr.
3. Rhwydweithiau mewnol yn cael eu diogelu'n gyson gan waliau tân caledwedd a meddalwedd ynghyd â sganio rheolaidd i ganfod a mynd i'r afael â bregusrwydd.
4. Mae dyfeisiadau cleientiaid a reolir gan Orbits yn cael eu diogelu gan feddalwedd gwrthfirws a meddalwedd diogelwch (Webroot).
5. Nid oes gan ddefnyddwyr safonol fynediad gweinyddol i ddyfeisiadau.
6. Mae traffig gwefan yn cael ei anfon drwy Systemau Enwi Parthau (DNS) ar gyfer hidlo yn ôl cynnwys a chategori yn ogystal â darparu seiber-ddiogelwch.
7. Darperir gwasanaethau cwmwl drwy Microsoft 365.

Mae Orbits IT yn prosesu ein data ac mae ein gwasanaethau cynorthwyo TG yn cael eu diffinio mewn contract ffurfiol a chytundeb lefel gwasanaeth (SLA). Mae'r contract a'r SLA yn cynnwys disgrifiadau o'r modd y mae Orbits IT'n sicrhau bod
a) ein data'n cael ei ddiogelu rhag bygythiad allanol a, b) bod yna drefniadau ar gyfer adennill data petai defnydd diawdurdod neu golled yn digwydd.

Fel ein prosesyddion data, mae gan Orbits IT ddyletswydd i roi gwybod i ni am unrhyw ddigwyddiad sy'n effeithio ar ddata personol. Petai yna ddigwyddiad sy'n effeithio ar ddata personol bydd Orbits IT yn adrodd hyn i un o'n prif swyddogion cyswllt drwy e-bost i'w ddilyn gan alwad ffôn - ein prif swyddogion cyswllt ar hyn o bryd yw San-Jin Park, Susan Crutcher neu Helen Verity.

Mae ymateb i ddefnydd diawdurdod o ddata'n dibynnu ar natur y digwyddiad. Bydd Orbits IT'n gweithio gyda staff Comisiynydd Cenedlaethau'r Dyfodol i benderfynu'r ymagwedd orau tuag at reoli hyn, a lleihau'r risg o ddefnydd diawdurdod/colled pellach. Gallai'r rhain gynnwys adfer data o ddyfeisiadau wrth gefn, a dadansoddi'r llwybr archwilio ar gyfer y data dan sylw.

Sut fedr defnydd diawdurdod/colled ddigwydd?

Gall defnydd diawdurdod o ddata/colli data ddigwydd mewn nifer o ffyrdd.

Systemau
Defnydd diawdurdod technegol allanol sy'n effeithio ar yr holl rwydwaith neu ar ran ohoni. Methiant technegol e.e. colli rhwydwaith, methu creu neu gopïo deunydd wrth gefn

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Pobl
Damweiniol e.e. clicio ar ddolen anhysbys, defnyddio ffon ddata anhysbys, lawrlwytho dogfen sydd heb ei gwirio, colli ffon ddata, ffôn symudol, gliniadur neu lechen.

Ein Hymagwedd ni
Mae ein polisïau a'n gweithdrefnau llywodraethu gwybodaeth wedi eu dylunio i leihau'r tebygrwydd o ddefnydd diawdurdod o ddata/colli data rhag digwydd, fodd bynnag, mae'n bwysig bod yr holl staff a chydweithwyr yn parhau i fod yn ymwybodol o'r risgiau.

Gall defnydd diawdurdod o ddata/colli data gael effeithiau arwyddocaol ar wrthrychau data (yn ein cynnwys ni i gyd). Fel corff cyhoeddus gallem gael ein dirwyo a cholli hyder y cyhoedd mewn modd arwyddocaol.

- Rydyn ni wedi adolygu ein trefniadau llywodraethu gwybodaeth ac wedi diweddaru ein polisïau a'n gweithdrefnau.
- Rydyn ni wedi penodi Swyddog Diogelu Data (DPO) i roi gwybodaeth ac arweiniad.
- Rydyn ni wedi rhoi gwybodaeth a sesiynau hyfforddi i'n staff a chydweithwyr.
- Rydyn ni wedi datblygu canllawiau i gynorthwyo staff wrth iddynt ymateb i ddefnydd diawdurod o ddata/colli data (Atodiad A).

Polisiau a Dogfennau Perthnasol

Polisi Llywodraethu Gwybodaeth

Polisi Diogelwch TG a Defnydd Derbyniol

Polisi Diogelu Gwybodaeth

Rhyddid Gwybodaeth (FOI) a Rheoliadau Gwybodaeth Amgylcheddol

Polisi Diogelu Data

Mynediad i Ganllawiau Gwybodaeth

Contract Rhannu Data a Chytundeb Lefel Gwasanaeth (SLA) gyda Orbits IT

Ffynonellau Cyngor ac Arweiniad:

Swyddog Diogelu Data (DPO) Sang-Jin Park

Swyddfa'r Comisiynydd Gwybodaeth – Cymru
2ail Lawr, Tŷ Churchill,
Ffordd Churchill, Caerdydd CF10 2HH
Ffôn: 029 2067 8400
Ffacs: 029 2067 8399
Ebost: wales@ico.org.uk <mailto:wales@ico.org.uk>

Gellir cael gwybodaeth bellach ar
www.ico.org.uk

Atodiad A: Ymateb i Ddefnydd Diawdurdod o Ddata/Colli Data: Sut i weithredu

Mae defnydd diawdurdod posibl* wedi digwydd: 1. Gwnewch unrhyw beth a fydd yn atal digwyddiad pellach o ddefnydd diawdurdod/colled neu a fydd yn lleihau eu heffaith 2. Rhowch wybod i uwch staff am ddefnydd diawdurdod o ddata/colli data 3. Gwiriwch ar unwaith gyda staff i sicrhau na fydd unrhyw gamau'n cael eu cymryd heb awdurdod a fedrai effeithio ar ddefnydd diawdurdod/colled	Nodwch ddyddiad ac amser y defnydd diawdurdod Nodwch unrhyw gamau a gymerwyd * Mae gan y rhai sy'n rheoli data ar y cyd, gyd-rwymedigaeth petai defnydd diawdurdod yn digwydd.
Gan weithio gyda Orbits IT aseswch: 1. Sut wnaeth y defnydd diawdurdod o ddata/colli data ddigwydd ac unrhyw gamau a gymerwyd i leihau effaith a lliniaru risgiau 2. Raddfa'r defnydd diawdurdod o ddata/colli data (math o wybodaeth a gafodd ei effeithio, maint y data) 3.Y posibilrwydd y gallai defnydd diawdurdod/colled golled ddigwydd eto 4. Yr effeithiau tebygol ar wrthrych/au data O hyn, nodwch unrhyw gamau pellach sy'n ofynnol	Cadwch nodiadau manwl cyfoes (i helpu i gwblhau adroddiad i ICO neu bwyllgor archwilio) Bydd camau pellach yn debygol o ddibynnu ar natur y defnydd diawdurdod a graddfa unrhyw golled. DS Gallai gweithredu maleisus neu fethiant i lynu wrth bolisi/gweithdrefnau arwain at gamau disgyblu. Ymgynghorwch â Hawliau Dynol am ba gamau i'w cymryd.

Os yn berthnasol – o fewn 72 awr – rhowch wybod i'r ICO am y defnydd diawdurdod gan roi'r wybodaeth ganlynol: 1. Dyddiad ac amser y digwyddiad 2.Sut y digwyddodd y defnydd diawdurdod/y golled 3. Graddfa'r defnydd diawdurdod o ddata/colli data 4. Posibilrwydd y bydd defnydd diawdurdod/colled yn digwydd eto 5. Yr effeithiau tebygol ar wrthrych/au data 6. Camau a gymerwyd hyd yn hyn i leihau colled bellach neu i leddfu effaith 7. Gweithredu pellach posibl yn y dyfodol (os caiff ei ganfod)	Aseswch yr effaith ar hawliau a rhyddid gwrthrychau data. Nodwch y math o wybodaeth a gaiff ei effeithio, maint y data. Cofnodwch eich penderfyniad i hysbysu neu beidio hysbysu. Sicrhewch eich bod yn cofnodi eich rhesymau dros beidio hysbysu. Defnyddiwch eich nodiadau a wnaed yn ystod y digwyddiad.
Os yn berthnasol rhowch wybod i Wrthrychau Data - heb oedi gormodol	Aseswch effaith ar hawliau a rhyddid gwrthrychau data. Cofnodwch eich penderfyniad i hysbysu neu beidio hysbysu. Sicrhewch eich bod yn nodi eich rhesymau dros beidio hysbysu. Defnyddiwch eich nodiadau a nodwyd yn ystod y digwyddiad.
Adrodd a Dysgu Mewnol - Beth fedrwn ni ei ddysgu o'r digwyddiad hwn? - Hyfforddiant pellach neu wybodaeth i staff? - Newid arferion mewnol neu weithdrefnau?	Crëwch gynllun gweithredu ar gyfer cyflawni camau o fewn 4-6 wythnos. Mae hyn hefyd yn rhoi tystiolaeth am benderfyniadau a wnaed a'r camau a gymerwyd.

Atodiad B: Adroddiad ar Ddefnydd Diawdurdod o Ddata/Colli Data

(Gwirioneddol/Bron â digwydd)

Adrodd digwyddiad o Ddefnydd Diawdurdod o Ddata/Colli Data	
Adroddwyd gan:	Dyddiad yr Adrodd:
Dyddiad y Digwyddiad:	Wedi digwydd neu bron â digwydd:

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Manylion (rhoi manylion am ddigwyddiad, camau a gymerwyd i leihau risgiau, Camau gofynnol pellach)
Cylchrediad

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Siambrau'r Farchnad, 5-7 Heol Eglwys Fair
Caerdydd, CF10 1AT
cystylltwchani@cenedlaethaurdyfodol.cymru
cenedlaethaurdyfodol.cymru

Future Generations Commissioner for Wales
Market Chambers, 5-7 St Mary Street
Cardiff, CF10 1AT
contactus@futuregenerations.wales
futuregenerations.wales