Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Polisi Diogelu Data

Datganiad Polisi

Mae Comisinydd Cenedlaethau'r Dyfodol wedi ymrwymo i sicrhau bod gwybodaeth yn cael ei rheoli'n dda yn unol â safonau arfer gorau ac mewn cydweithrediad â dyletswyddau cyfreithiol y Comisiynydd o dan y Ddeddf Diogelu Data (DPA), a'r Rheoliad Cyffredinol ar Reoli Data (GDPR), a Rheoliadau Preifatrwydd a Chyfathrebu Electronig (PECR).

Mae'r GDPR yn dod i rym ar 25 Mai 2018; Dylai Deddf Diogelu Data newydd ddod yn gyfraith yn ystod 2018. Mae'r newidiadau i reoliadau diogelu data wedi eu gwneud yn ofynnol i ni adolygu a diwygio ein hymagwedd tuag at reoli gwybodaeth bersonol.

Mae'r polisi hwn yn berthnasol i'n defnydd o wybodaeth bersonol h.y. gwybodaeth sy'n adnabod neu sy'n ymwneud ag unigolyn byw. Fel corff cyhoeddus mae rheoli gwybodaeth yn dda yn fater o ymddiriedaeth gyhoeddus; mae gennym gyfrifoldeb i ddiogelu data personol sy'n cael ei gadw gennym ac i'w brosesu a'i rannu mewn dull cyfreithiol.

Cyfrifoldebau

Mae'r Comisiynydd yn disgwyl i'r holl staff a chydweithwyr gydymffurfio â gofynion y polisi hwn.

Mae gan Gyfarwyddwr Cyllid a Llywodraethu Corfforaethol (Helen Verity) gyfrifoldeb cyffredinol am Ddiogelu Data a hi yw'r un a enwir fel Rheolwr Data.

Mae'r GDPR yn ei gwneud yn ofynnol i ni enwi Swyddog Diogelu Data.

Ein Swyddog Diogelu Data yw San-Jin Park; bydd y Swyddog Diogelu Data'n monitro cydymffurfio o ddydd i ddydd, gan roi cyngor ac arweiniad i staff ar faterion Diogelu Data a materion preifat. Mae'r Swyddog Diogelu Data hefyd yn gyfrifol am gyfathrebu ar ein rhan â Swyddfa'r Comisiynydd Gwybodaeth parthed hysbysu prosesu, colli data neu ddefnydd diawdurdod a chwynion.

Mae'r Pwyllgor Archwilio'n cadw'r oruchwyliaeth dros gydymffurfio â Diogelu Data. Caiff unrhyw faterion Diogelu Data eu trafod (fel eitem sefydlog) mewn cyfarfodydd ARAC yn chwarterol.

Dangos Cydymffurfiad

I sicrhau ein bod yn parhau i gydymffurfio â diogelu data mae'r GDPR wedi cymryd y camau dilynol:

- Rydyn ni wedi gweithredu mesurau technegol a sefydliadol priodol sy'n sicrhau ac yn dangos ein bod yn cydymffurfio. Mae hyn yn cynnwys ein hadolygiad o bolisïau

llywodraethu gwybodaeth a gweithgareddau prosesu, archwiliadau mewnol, adolygiadau o bolisïau a gweithdrefnau mewnol Adnoddau Dynol a hyfforddi staff.

- Rydyn ni'n cadw dogfennau perthnasol ar ein gweithgareddau prosesu.

- Rydyn ni wedi enwi swyddog diogelu data penodedig
- Rydyn ni wedi gweithredu ymagwedd 'preifatrwydd drwy ddyluniad'

Egwyddorion Diogelu Data

Mae Egwyddorion GDPR yn debyg i'r 8 Egwyddor Diogelu Data gwreiddiol ac wedi eu cynnwys yn llawn yn Atodiad A. Mae'r GDPR yn nodi bod y Rheolwr Data'n gyfrifol am gydymffurfio â'r egwyddorion hyn.

Yn fyr mae Egwyddorion GDPR yn datgan y bydd data personol:

- Yn cael ei brosesu mewn dull cyfreithiol a theg mewn ffordd dryloyw i unigolion perthnasol
- Yn cael ei gasglu ar gyfer dibenion penodol, pendant a chyfreithiol heb gael ei brosesu ymhellach mewn modd sy'n anghydnaws â'r dibenion hynny
- Yn ddigonol, yn berthnasol a chyfyngedig i'r diben y'i proseswyd ar ei gyfer
- Yn gywir ac wedi ei diweddaru; gwybodaeth anghywir i gael ei dileu neu ei chywiro ar fyrder
- Ei gadw ar ffurf nad yw'n caniatáu adnabod gwrthrychau data yn hwy nag sydd ei angen
- Yn defnyddio mesurau technegol a sefydliadol priodol i ddiogelu hawliau a rhyddid unigolion
- Yn prosesu'n ddiogel ac yn erbyn colled ddamweiniol, distryw neu niwed, gan ddefnyddio mesurau technegol sefydliadol priodol

Diffiniadau Allweddol

Gwrthrych Data – yr unigolyn sy'n wrthrych y data

Rheolwr Data – sy'n penderfynu'r dibenion a'r dulliau o brosesu'r data

Prosesydd Data – sy'n gyfrifol am brosesu data personol ar ran y rheolwr

Data personol - unrhyw wybodaeth sy'n berthnasol i berson a enwir (gwrthrych y data), gall hyn gynnwys yr enwau a'r cyfeiriadau amlwg yn ogystal â chyfeiriadau e-bost a delweddau.

Data categori arbennig (data personol sensitif)

- Mae data categori arbennig yn fwy sensitif felly mae'n gofyn am fwy o ddiogelwch.
- Mae hyn yn cynnwys gwybodaeth am hil unigolyn, gwreiddiau ethnig, gwleidyddiaeth, crefydd, aelodaeth o undeb llafur, geneteg, biometreg (lle caiff ei ddefnyddio at ddibenion TG), iechyd, bywyd rhywiol neu gyfeiriadedd rhywiol.
- Gallai colli neu danseilio'r math hwn o ddata achosi risgiau mwy arwyddocaol i hawliau neu ryddid cyffredinol person e.e. eu rhoi mewn risg o ddioddef gwahaniaethu.
- I brosesu data categori arbennig rhaid i ni fodloni amodau arbennig y GDPR.

Preifatrwydd drwy Ddylunio, ac Asesiadau o Effaith Preifatrwydd ar Ddiogelu Data (DPIA)
Mae gennym ddyletswydd i weithredu mesurau (technegol a sefydliadol) i ddangos ein bod wedi ystyried ac integreiddio data i mewn i'n gweithgareddau prosesu. Er enghraifft, yng nghyfnod cynllunio prosiect partneriaeth newydd byddwn yn ystyried materion Diogelu Data. Gall y bydd prosiectau cymhleth yn gofyn am Asesiad o Effaith Preifatrwydd Diogelu Data (DPIA). Bydd ein Swyddog Diogelu Data'n ein cynghori pan fydd hyn yn ofynnol.

Gellir cael mwy o wybodaeth yn Atodiad C

Cytundebau Rhannu Data gall y bydd y rhain yn addas mewn amgylchiadau arbennig ac mae Cytundeb Rhannu Gwybodaeth Bersonol Cymru (WASPI) yn darparu templed y gellir ei addasu lle mae nifer o sefydliadau'n dymuno rhannu gwybodaeth bersonol. Gall ein Swyddog Diogelu Data gynghori ar ba bryd y gallai hyn fod yn addas ac ar addasu'r templed.

Sail Gyfreithiol ar gyfer prosesu – mae'n rhaid i ni fod wedi adnabod sail gyfreithiol ddilys ar gyfer unrhyw brosesu cyn i'r prosesu gychwyn. Er enghraifft, caniatâd yw un sail gyfreithiol, fodd bynnag, mae'r GDPR yn gosod safonau uchel ar gyfer caniatâd, a dylem ystyried a yw sail arall ar gyfer prosesu'n fwy addas.

Hawliau Unigolyn
Mae ymagwedd tuag at ddiogelu data'n dibynnu arnom ni i gyflawni cyfrifoldebau a dyletswyddau rheolwr data. Mae angen i ni ystyried hawliau a rhyddid unigolion wrth i ni gyflawni ein gwaith. Mae'r GDPR yn ymestyn hawliau unigolyn mewn perthynas â'u data; cynhwysir eglurhad llawn o'r hawliau hyn yn Atodiad D.

Fodd bynnag, y rhai hyn yw'r rhai sydd fwyaf perthnasol i ni:

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Yr hawl i gael gwybodaeth – mae'n rhaid i ni ddweud wrth unigolion am y modd yr ydym yn prosesu eu data a sut i gysylltu â ni i arfer eu hawliau. Rydyn ni'n defnyddio Hysbysiad Preifatrwydd i wneud hyn.

Hawl i fynediad – mae hyn yn rhoi hawl i unigolyn gael copi o'r data sydd gennym, y cyfeirir ato hefyd fel 'cais gwrthrych i gael mynediad'.

Hawliau i gywiriad (cywiriad neu gwblhad data personol anghywir), dileu (y cyfeirir ato hefyd fel yr hawl i gael ei anghofio) a'r hawl i wrthwynebu prosesu neu i brosesu gael ei gyfyngu.

Rhaid i ni ddarparu ymateb i'r cais am hawliau o fewn **20 niwrnod**.

Colli Data a Defnydd Diawdurdod

Drwy ein polisïau a gweithdrefnau Llywodraethu Gwybodaeth rydyn ni wedi sefydlu fframwaith ar gyfer trin gwybodaeth yn effeithiol. Rydyn ni wedi gosod yn eu lle'r mesurau technegol a sefydliadol i amddiffyn yn addas ddata personol yr ydym yn ei gadw.

Fodd bynnag, mae'r risg y bydd yna ddigwyddiad diogelwch sy'n effeithio ar gyfrinachedd, cywirdeb neu argaeledd data personol yn parhau. Mae defnydd diawdurdod o ddata personol yn golygu defnydd diawdurdod o ddiogelwch gan arwain at ddinistr damweiniol neu anghyfreithlon, colli data, newid, datgeliad diawdurdod neu fynediad i ddata personol. Mae hyn yn cynnwys defnydd diawdurdod sy'n dod yn sgil achosion bwriadol a damweiniol.

Mae'n hollbwysig felly eich bod yn ymwybodol o'ch cyfrifoldeb i adrodd colli data posibl neu ddefnydd diawdurdod yn syth ar ôl i chi ddod yn ymwybodol ohono.

Gall defnydd diawdurdod o ddata personol gynnwys:

- Mynediad gan drydydd parti heb awdurdod
- Gweithredu bwriadol neu ddamweiniol (neu ddiffyg gweithredu)
- Anfon data personol at y derbynnydd anghywir
- Dyfeisiadau'n cynnwys data personol yn cael eu colli neu eu dwyn
- Newid data personol heb ganiatâd
- Colli argaeledd data personol

Mae'r GDPR yn gosod dyletswydd ar sefydliadau i adrodd rhai mathau o ddefnydd diawdurdod o ddata personol i'r Swyddfa'r Comisiynydd Gwybodaeth o Fewn 72 awr a phetai'r defnydd diawdurdod yn digwydd effeithio'n arwyddocaol ar unigolion rhaid i ni roi gwybod iddynt heb

oedi. Gallai sefydliad gael dirwy sylweddol am ddefnydd diawdurdod difrifol ac am fethu adrodd ar ddefnydd diawdurdod yn ôl y gofyn.

Gan weithio gyda IT Support Orbits IT, rydyn ni wedi gosod yn eu lle ddulliau cadarn o ganfod defnydd diawdurdod.

Mae ein Polisi Defnydd Diawdurdod o Ddata/Colli Data yn rhoi manylion am y camau sy'n rhaid i ni eu cymryd petai defnydd diawdurdod o ddata/colli data'n digwydd.

Rydyn ni wedi clustnodi cyfrifoldeb am archwilio'r posibilrwydd o defnydd diawdurdod o ddata/colli data i'r Swyddog Diogelu Data.

Rheoliadau Preifatrwydd a Chyfathrebu Electronig (PECR)

Mae PECR yn gweithio ochr yn ochr â diogelu data ac mae'n cwmpasu gweithgaredd marchnata electronig dros y ffôn, ffacs, e-bost, testun neu unrhyw fath arall o bostio electronig. Nid yw'r GDPR yn disodli PECR ac mae angen i ni gydymffurfio â'r ddau mewn unrhyw weithgaredd marchnata uniongyrchol.

Diogelu Gwybodaeth Bersonol - Cofiwch wneud rhai pethau a pheidiwch â gwneud pethau eraill

Cofiwch – gyfarwyddo ag egwyddorion y GDPR

Cofiwch – gyfarwyddo â hawliau unigol o dan y GDPR – eich hawliau chi yw'r rhain hefyd

Cofiwch – ystyried materion preifatrwydd fel rhan o'ch dylunio prosiect cychwynnol

Cofiwch – feddwl am sail gyfreithiol ar gyfer unrhyw brosesu data personol cyn i chi gychwyn prosesu

Cofiwch – feddwl am eich gweithgareddau o ddydd i ddydd a lle gallai risgiau preifatrwydd godi e.e. ydych chi'n anfon e-byst ymlaen yn rheolaidd heb ddweud yn gyntaf wrth yr un â greodd yr e-bost?

Cofiwch – chwilio am gyngor oddi wrth y Swyddog Diogelu Data mewn cyfnod cynnar

Peidiwch – â rhannu gwybodaeth bersonol os oes gennych unrhyw amheuon am ddiogelwch gwneud hynny. Cysylltwch â'r Swyddog Diogelu Data a gwnewch yn siŵr eich bod yn cydymffurfio â'r GDPR.

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

Peidiwch – gohirio adrodd problem – posibilrwydd o golli data/defnydd diawdurdod. Gall adrodd yn gynnar atal mater rhag gwaethygu.

Ffynonellau Cyngor ac Arweiniad

Gall ein Swyddog Diogelu Data (DPO) ddarparu cyngor ac arweiniad mewn perthynas â materion cydymffurfio'n ymwneud â diogelu data o ddydd i ddydd.

Mae Swyddfa'r Comisiynydd Gwybodaeth wedi cyhoeddi ac yn parhau i ddiweddaru arweiniad manwl ar gydymffurfio â'r GDPR.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Polisïau Perthnasol

Polisi Llywodraethu Gwybodaeth

Polisi Diogelwch TG & Defnydd Derbyniol

Polisi Diogelwch Gwybodaeth

Rhyddid Gwybodaeth & Pholisi Rheoliadau Amgylcheddol

Mynediad i Ganllawiau ar Wybodaeth

Polisi Defnydd Diawdurdod o Ddata

Atodiad A: Egwyddorion GDPR.

Mae Erthygl 5 y GDPR yn ei gwneud yn ofynnol i ddata personol:

a) gael ei brosesu'n gyfreithlon, yn deg ac mewn dull tryloyw mewn perthynas ag unigolion;
b) gael ei gasglu at ddibenion penodol, clir a chyfreithiol heb ei brosesu ymhellach mewn dull sy'n anghydfynd â'r dibenion hynny; ni chaiff prosesu pellach at ddibenion archifo er budd y cyhoedd, dibenion ymchwil hanesyddol neu ddibenion ystadegol eu hystyried fel rhai sy'n anghydfynd â'r dibenion cychwynnol.

c) fod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol i'r dibenion y'i proseswyd ar eu cyfer.

d) fod yn gywir, a lle mae hynny'n angenrheidiol, gael ei ddiweddaru; rhaid cymryd pob cam rhesymol i sicrhau bod data personol sy'n anghywir, o gadw mewn golwg y dibenion y'i proseswyd ar eu cyfer, yn cael ei ddileu neu ei gywiro yn ddi-oed.

e) gael ei gadw mewn ffurf nad yw'n caniatáu adnabod gwrthrychau data yn hwy nag sydd ei angen at y dibenion y'i proseswyd ar eu cyfer; gellir cadw data personol am gyfnodau hwy cyn belled â bod y data personol yn cael ei brosesu yn unig at ddibenion archifo er lles y cyhoedd, ymchwil wyddonol neu hanesyddol neu ddibenion sefydliadol neu ddibenion ystadegol yn amodol ar weithrediad y mesurau priodol technegol a sefydliadol sy'n ofynnol gan y GDPR er mwyn diogelu hawliau a rhyddid unigolion, a

f) chael ei brosesu mewn dull sy'n sicrhau diogelu data personol mewn dull priodol, yn cynnwys ei ddiogelu yn erbyn colled ddamweiniol, dinistr neu niwed, gan ddefnyddio mesurau technegol neu sefydliadol priodol.

Mae Erthygl 5(2) yn ei gwneud yn ofynnol:
- i'r rheolwr fod yn gyfrifol am, ac yn medru dangos, cydymffurfiad â'r egwyddorion

Atodiad B - Rheoli Gweithdrefn Cais am Wybodaeth Bersonol (SAR)

- Cofnodi cais a dderbyniwyd
- Trosglwyddo i DPO
- Agor ffeil a defnyddio rhif cyfeirnod unigryw
- Nodi ymateb yn ôl dyddiad – 20 niwrnod ar ôl ei dderbyn
- Egluro cais - cwmpas
- Gwirio hunaniaeth
- Holl e-byst staff â dyddiad ymateb
- Casglu gwybodaeth
- Gwirio cynnwys 3ydd parti
- Paratoi ymateb i wrthrych y data
- Gwirio cynnwys
- Ymateb i wrthrych data o fewn 20 niwrnod.

Ymateb i geisiadau eraill seiliedig ar hawliau

- Cais am Gofnod
- Trosglwyddo i DPO
- Agor ffeil a defnyddio rhif cyfeirnod unigryw
- Gwirio hunaniaeth
- Adnabod gwybodaeth/prosesu
- Egluro cais os ydyw hynny'n angenrheidiol
- Gweithredu cywiriad/dilead
- Cofnodi gweithred
- Cadarnhau'r camau a gymerwyd i wrthrych y data
- Cau ffeil

Atodiad C - Egwyddorion Preifatrwydd drwy ddylunio

1. Rhaid cael ymagwedd sy'n mabwysiadu safiad rhagweithiol yn hytrach nag adweithiol ac anelu at atal risgiau preifatrwydd yn hytrach na mynd i'r afael â hwynt ar ôl iddynt ddigwydd.
2. Caiff preifatrwydd ei ddefnyddio fel rhagosodiad
3. Rhaid i breifatrwydd gael ei sefydlu mewn dylunio
4. Mae Preifatrwydd drwy Ddylunio yn sicrhau gweithrediad llwyr ac mae'n ceisio cyflawni preifatrwydd a diogelwch
5. Rhaid i ddiogelwch gael ei wneud yn rhan integredig o'r systemau drwy eu holl gylch bywyd
6. Mae'n ymroi i wireddu gweledegd a thryloywder
7. Mae defnyddwyr i gael lle canolog mewn systemau a rhaid talu sylw i fuddiannau ac anghenion defnyddwyr.

Atodiad D - Hawliau Unigol o dan GDPR.

Yr hawl i dderbyn gwybodaeth – mae gan unigolion hawl i gael gwybodaeth am gasglu data a'r defnydd a wneir o'u data. Mae hwn yn ofyniad allweddol o dryloywder o dan y GDPR. Rydyn ni'n defnyddio Hysbysiad Preifat i wneud hyn.

Hawl i gael mynediad – mae gan unigolion yr hawl i gyrchu eu data personol. Mae'r hawl hwn yn caniatáu i unigolion fod yn ymwybodol o, a gwirio cyfreithlondeb y prosesu.

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Hawl i gywiro - mae gan unigolion yr hawl i gael eu data personol anghywir wedi ei gywiro neu ei gwblhau os nad yw'n gyflawn.

Yr hawl i ddileu - mae gan unigolion yr hawl i gael eu data personol wedi ei ddileu (y cyfeirir ato hefyd fel hawl i gael ei anghofio). Nid yw'r hawl hwn yn absoliwt ac mae'n berthnasol yn unig o dan amgylchiadau arbennig.

Yr hawl i gyfyngu ar brosesu – mae gan unigolion yr hawl i ofyn am gyfyngu neu roi terfyn ar brosesu eu data personol. Nid yw'r hawl hwn yn absoliwt ac mae'n berthnasol yn unig o dan amgylchiadau arbennig.

Hawl i gludo data – mae'r hawl hwn yn caniatáu i unigolion gael eu data personol ar gyfer eu defnydd hwy eu hunain ar draws gwahanol wasanaethau.

Hawl i wrthwynebu – mae gan unigolion yr hawl i wrthwynebu prosesu seiliedig ar fudd cyfreithlon neu berfformiad tasg sydd o fudd i'r cyhoedd; marchnata uniongyrchol a phrosesu er budd ymchwil wyddonol/hanesyddol ac ystadegau.

Hawliau sy'n berthnasol i wneud penderfyniadau awtomataidd a phroffilio – mae'n rhaid i unigolion sy'n agored i'r math hwn o brosesu gael gwybodaeth am y prosesu a chael dulliau syml o wneud cais am ymyrraeth ddynol neu herio penderfyniad.

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