



Polisi Diogelu Data

Mae'r polisi hwn yn cyflwyno gwybodaeth am y ddeddfwriaeth diogelu data, gan gynnwys Rheoliad Cyffredinol y DU ar Ddiogelu Data (yr 'UK GDPR') a Deddf Diogelu Data 2018, y mae'n rhaid i Gyngor Gweithredu Gwirfoddol Cymru ('ni', 'ein') gydymffurfio â nhw.

Mae'r polisi hwn yn berthnasol i'r holl aelodau staff, ymddiriedolwyr, gwirfoddolwyr a phobl eraill sy'n gweithio i ni.

Mae'r polisi hwn yn rhoi trosolwg cyffredinol o'r gofynion cyfreithiol. Mae'n amlinellu'r hyn rydym yn ei ddisgwyl gennych o ran trin gwybodaeth bersonol, waeth ar ba fformat y caiff ei storio. Mae hyn yn cynnwys gwybodaeth am:

- Gyflogeion a gweithwyr ac ymgeiswyr cyfredol neu flaenorol
- Gwirfoddolwyr ac ymgeiswyr cyfredol neu flaenorol
- Ymddiriedolwyr ac ymgeiswyr cyfredol neu flaenorol
- Buddiolwyr / cleientiaid / defnyddwyr ein gwasanaethau
- Defnyddwyr ein sianeli cyfryngau ar-lein a digidol
- Cefnogwyr, rhoddwyr a chyllidwyr cyfredol, blaenorol neu bosibl, gan gynnwys unigolion a chynrychiolwyr mudiadau
- Pobl yr ydym yn ymgysylltu â nhw o ran ein gweithgarwch ymgyrchu
- Cynrychiolwyr mudiadau yr ydym mewn partneriaethau neu'n cydweithio â nhw
- Cynrychiolwyr ein cyflenwyr

Mae'n rhaid i chi ddarllen, deall a chydymffurfio â'r polisi hwn wrth drafod gwybodaeth bersonol ar ein rhan a mynychu unrhyw hyfforddiant gorfodol ar y gofyniad hwn. Gall y polisi gael ei ategu gan ganllawiau penodol sy'n berthnasol i'ch rôl.

Mae'n orfodol eich bod yn cydymffurfio â'r polisi hwn. Os torrir unrhyw ran o'r polisi hwn, gallai arwain at gamau disgyblu.

1. DIFFINIADAU

Defnyddir y diffiniadau canlynol yn y polisi hwn:

Asesiad o'r Effaith ar Breifatrwydd Data (DPIA)	Adnodd ac asesiad a ddefnyddir i nodi a lleihau risgiau gweithgareddau prosesu data. Gellir cynnal DPIA fel rhan o Breifatrwydd trwy Ddyluniad a dylid ei gynnal ar gyfer pob rhaglen newid system neu fusnes fawr sy'n cynnwys y dasg o brosesu Data Personol
Creu neu osod ffugenw	Amnewid gwybodaeth a allai ddatgelu pwy yw unigolyn, naill ai'n uniongyrchol neu'n anuniongyrchol, am un neu ragor o ddynodwyr neu ffugenwau artiffisial fel na ellir adnabod y sawl y mae'r data'n berthnasol iddo heb ddefnyddio gwybodaeth ychwanegol a ddylai gael ei chadw ar wahân ac yn ddiogel
Data Personol	Unrhyw wybodaeth sy'n nodi Testun Data neu wybodaeth sy'n ymwneud â Thestun Data y gallem adnabod y Testun Data ohoni (yn uniongyrchol neu'n anuniongyrchol), waeth a fydd hynny'n digwydd drwy'r data hwnnw yn unig neu drwy gyfuniad o nodweddion adnabod eraill sydd gennym yn ein meddiant neu y gallem gael mynediad rhesymol atynt. Mae Data Personol yn cynnwys Data Personol Categori Arbennig a Data Personol dan Ffugenw, ond nid yw'n cynnwys data dienw na data lle mae enw unigolyn wedi ei ddileu'n barhaol. Gall data personol fod yn ffeithiol (er enghraifft, enw, cyfeiriad e-bost, lleoliad neu ddyddiad geni) neu'n farn am weithrediadau neu ymddygiad unigolyn

Data Personol Categori Arbennig	Gwybodaeth sy'n datgelu tarddiad hiliol neu ethnig, safbwyntiau gwleidyddol, credoau crefyddol neu debyg, aelodaeth o undeb llafur, cyflyrau iechyd corfforol neu feddyliol, bywyd rhywiol, cyfeiriadedd rhywiol, data biometrig neu enetig, a gwybodaeth sy'n ymwneud â throseddau ac euogfarnau
Hysbysiad Preifatrwydd	Hysbysiad yw hwn sy'n amlinellu'r wybodaeth y dylid ei rhoi i Destunau Data pan fyddwn yn casglu gwybodaeth amdanynt
Preifatrwydd trwy Ddyluniad	Rhoi mesurau technegol a sefydliadol priodol ar waith mewn modd effeithiol er mwyn sicrhau cydymffurfiaeth â'r ddeddfwriaeth diogelu data
Prosesu neu Broses	Mae hyn yn golygu unrhyw weithgaredd sy'n ymwneud â defnyddio Data Personol. Mae'n cynnwys cael, cofnodi neu ddal y data, neu gyflawni unrhyw weithrediad neu set o weithrediadau ar y data, gan gynnwys trefnu, diwygio, adalw, defnyddio, datgelu, dileu neu ddinistrio'r data. Mae prosesu hefyd yn cynnwys anfon neu drosglwyddo Data Personol i drydydd partiön
Prosesyddion Data	Unrhyw drydydd parti rydym yn ei ddefnyddio i Brosesu Data Personol ar ein rhan
Rheolydd	Dyma'r unigolyn neu fudiad sy'n pennu pryd, pam a sut i brosesu Data Personol. Ni yw'r Rheolydd Data ar gyfer yr holl Ddata Personol a ddefnyddir yn ein mudiad at ein dibenion ein hunain
Swyddog Diogelu Data (DPO)	Yr unigolyn sy'n gyfrifol am gydymffurfiaeth diogelu data o fewn eich mudiad. Ar hyn o bryd, yr unigolyn hwn yw Matthew Brown, Cyfarwyddwr Gweithrediadau

Testun Data	Yr unigolyn byw, adnabyddedig neu adnabyddadwy y mae gennym Ddata Personol amdano
--------------------	---

Torri Data Personol	Mae hwn yn golygu unrhyw weithred neu hepgoriad sy'n peryglu diogelwch, cyfrinachedd, cywirdeb neu argaeledd Data Personol neu'r camau diogelu ffisegol, technegol, gweinyddol neu sefydliadol yr ydym ni neu ein darparwyr gwasanaeth trydydd parti yn eu rhoi ar waith i'w ddiogelu. Mae colli, neu fynediad, datgeliad neu gaffaeliad anawdurdodedig o Ddata Personol yn achos o Dorri Data Personol
----------------------------	---

2. EGWYDDORION DIOGELU DATA

Yn ôl y gyfraith, mae'n rhaid i Ddata Personol:

- gael ei brosesu'n gyfreithlon, yn deg ac mewn modd tryloyw
- cael ei gasglu at ddibenion penodol, pendant a chyfreithlon yn unig
- bod yn ddigonol, yn berthnasol ac wedi ei gyfyngu at yr hyn sy'n angenrheidiol mewn perthynas â'r dibenion y mae'n cael ei brosesu
- bod yn gywir a'i gadw'n gyfredol pan fydd angen
- peidio â chael ei gadw ar ffurf sy'n caniatáu i Destunau Data gael eu hadnabod am hirach nag sydd ei angen at y dibenion y mae'r data yn cael ei brosesu
- cael ei brosesu mewn modd sy'n sicrhau ei ddiogelwch gan ddefnyddio mesurau technegol a sefydliadol priodol i'w ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon a rhag colled, distryw neu ddifrod damweiniol.

Rhaid hefyd peidio â throsglwyddo Data Personol y tu allan i CGGC heb sicrhau bod mesurau diogelu priodol ar waith.

Mae gofyniad arnom i alluogi Testunau Data i arfer hawliau penodol mewn perthynas â'u Data Personol.

Mae'n rhaid i ni hefyd gydymffurfio â gofynion cyfreithiol penodol pan fydd gan gyflenwyr sy'n darparu gwasanaethau ar ein cyfer fynediad at

Ddata Personol a phan fyddwn yn gweithio gyda mudiadau ac angen rhannu Data Personol.

Rydym yn gyfrifol am gydymffurfio â'r gofynion o dan y gyfraith (atebolrwydd) ac mae'n rhaid i ni allu dangos ein bod yn cydymffurfio â'r gofynion hyn.

3. CYFREITHLONDEB A THEGWCH

Mae'n rhaid prosesu data personol yn gyfreithlon, yn deg ac mewn modd tryloyw mewn perthynas â'r Testun Data.

Gallwch ddim ond casglu, prosesu a rhannu Data Personol yn deg ac yn gyfreithlon ac at ddibenion penodol. Mae'r gyfraith yn cyfyngu ein gweithrediadau o ran Data Personol at ddibenion cyfreithlon penodol. Nid diben y cyfyngiadau hyn yw atal prosesu. Yn hytrach, eu nod yw sicrhau ein bod yn prosesu Data Personol mewn modd teg, heb effeithio'n niweidiol ar y Testun Data.

Dyma'r seiliau cyfreithlon sydd ar gael wrth brosesu data personol categori anarbennig:

- mae'r Testun Data wedi rhoi caniatâd i gael ei (d)data personol wedi ei brosesu at un neu ragor o ddibenion penodol
- mae'r prosesu'n angenrheidiol ar gyfer perfformiad contract rhyngom ni a'r Testun Data neu er mwyn cymryd camau ar gais y Testun Data cyn taro bargaen
- mae'r prosesu'n angenrheidiol er mwyn cydymffurfio â rhwymedigaeth gyfreithiol yr ydym yn rhwym iddi
- mae'r prosesu'n angenrheidiol er mwyn diogelu buddiannau hollbwysig y Testun Data neu unigolyn naturiol arall
- mae'r prosesu'n angenrheidiol ar gyfer perfformiad tasg a gyflawnir er budd y cyhoedd
- mae'r prosesu'n angenrheidiol at ddibenion buddiannau cyfreithlon yr ydym yn anelu atynt neu y mae trydydd parti yn anelu atynt, ac eithrio pan fydd buddiannau neu hawliau a rhyddidau sylfaenol y Testun Data yn bwysicach na buddiannau o'r fath a bod angen diogelu data personol, yn arbennig pan mai plentyn yw'r Testun Data.

Mae amrediad o ofynion cyfreithiol ychwanegol yn berthnasol wrth brosesu data personol categori arbennig. Mae angen un o'r seiliau cyfreithlon a nodwyd uchod, ynghyd â sail gyfreithlon ar wahân o'r rhestr ganlynol:

- mae'r testun data wedi rhoi **caniatâd pendant** i gael y data personol hwnnw wedi ei brosesu at un neu ragor o ddibenion penodol, ac eithrio pan fydd cyfraith yr Undeb neu'r aelod-wladwriaeth yn nodi na all y gwaharddiad y cyfeirir ato ym mharagraff 1 gael ei godi gan y testun data;
- mae'r prosesu'n angenrheidiol at ddibenion cyflawni rhwymedigaethau ac arfer hawliau penodol y rheolydd neu'r testun data yn y maes cyfraith cyflogaeth a nawdd cymdeithasol ac amddiffyniad cymdeithasol, cyhyd â'i fod wedi ei awdurdodi gan gyfraith Undeb neu aelod-wladwriaeth neu gan gytundeb cyfunol yn unol â chyfraith aelod-wladwriaeth sy'n darparu ar gyfer mesurau diogelu priodol ar gyfer hawliau a buddiannau priodol y testun data;
- mae'r prosesu'n angenrheidiol i amddiffyn buddiannau hollbwysig y testun data neu unigolyn naturiol arall lle na all y testun data roi caniatâd, yn gorfforol neu'n gyfreithiol
- mae'r prosesu yn cael ei wneud wrth gyflawni ei weithgareddau cyfreithlon gyda mesurau diogelu priodol gan fudiad, cymdeithas neu unrhyw gorff nid-er-elw arall â nod gwleidyddol, athronyddol, crefyddol neu undeb llafur, ac ar yr amod bod y prosesu'n ymwneud ag aelodau neu gyn-aelodau'r corff yn unig neu ag unigolion sydd â chysylltiad rheolaidd ag ef mewn cysylltiad â'i ddibenion ac nad yw'r data personol yn cael ei ddatgelu y tu allan i'r corff hwnnw heb ganiatâd y testunau data
- mae'r prosesu yn ymwneud â data personol sy'n amlwg yn cael ei wneud yn gyhoeddus gan y testun data
- mae'r prosesu'n angenrheidiol ar gyfer sefydlu, arfer neu amddiffyn honiadau cyfreithiol neu bryd bynnag y bydd llysoedd yn ymddwyn yn rhinwedd eu gwaith barnwrol
- mae'r prosesu'n **angenrheidiol at resymau budd cyhoeddus sylweddol**, ar sail cyfraith Undeb neu aelod-wladwriaeth a fydd yn gymesur â'r nod yr anelir ato, yn parchu hanfod yr hawl i ddiogelu data ac yn darparu ar gyfer

mesurau addas a phenodol i amddiffyn hawliau a buddion sylfaenol y testun data

- mae'r prosesu'n angenrheidiol at ddibenion meddyginiaeth ataliol neu alwedigaethol, ar gyfer asesu gallu'r cyflogai i weithio, cael diagnosis meddygol, darparu iechyd neu ofal cymdeithasol neu driniaeth neu i reoli systemau a gwasanaethau iechyd neu ofal cymdeithasol **ar sail cyfraith Undeb neu aelod-wladwriaeth neu yn unol â contract** gyda gweithiwr iechyd proffesiynol ac yn unol â'r amodau a'r camau diogelu y cyfeiriwyd atynt ym mharagraff 3
- mae'r prosesu'n angenrheidiol am resymau budd cyhoeddus ym maes iechyd cyhoeddus, fel amddiffyn rhag bygythiadau trawsffiniol difrifol i iechyd neu sicrhau safonau uchel mewn ansawdd a diogelwch gofal iechyd a safonau cynnyrch meddyginiaethol neu ddyfeisiau meddygol, ar sail cyfraith Undeb neu aelod-wladwriaeth sy'n darparu ar gyfer mesurau addas a phenodol i amddiffyn hawliau a rhyddidau y Testun Data
 - mae prosesu'n angenrheidiol ar gyfer archifo dibenion er budd y cyhoedd, dibenion ymchwil gwyddonol neu hanesyddol neu ddibenion ystadegol, yn unol ag [Erthygl 89 \(Saesneg yn unig\) \(1\)](#) ar sail cyfraith Undeb neu aelod-wladwriaeth a fydd yn gymesur â'r nod yr anelir ato, yn parchu hanfod yr hawl i ddiogelu data ac yn darparu ar gyfer mesurau addas a phenodol i amddiffyn hawliau a buddion sylfaenol y testun data

4. TRYLOYWDER

Mae'r gyfraith yn gofyn i ni roi gwybodaeth fanwl, benodol am ein defnydd o Ddata Personol i Destunau Data. Mae'n rhaid i wybodaeth o'r fath gael ei darparu drwy Hysbysiadau Preifatrwydd priodol sy'n gorfod bod yn gryno, yn dryloyw, yn ddealladwy, yn hawdd eu cyrchu ac mewn iaith glir a phlaen fel y gall y Testun Data eu deall yn hawdd.

Pryd bynnag rydym yn casglu Data Personol gan Destunau Data'n uniongyrchol, mae'n rhaid i ni roi gwybodaeth i'r Testun Data sy'n cynnwys pwy ydym ni a sut a pham y byddwn yn Prosesu, datgelu, diogelu ac yn cadw ei Ddata Personol. Gwneir hyn drwy Hysbysiad Preifatrwydd sy'n

gorfod cael ei gyflwyno y tro cyntaf y bydd y Testun Data yn darparu'r Data Personol.

Pan gaiff Data Personol ei gasglu'n anuniongyrchol (er enghraifft, gan drydydd parti neu drwy ffynhonnell sydd ar gael yn gyhoeddus), mae'n rhaid i ni roi gwybodaeth yr Hysbysiad Preifatrwydd i'r Testun Data cyn gynted â phosibl, ond dim hwyrach nag un mis ar ôl casglu/derbyn y data. Mae'n rhaid i ni hefyd wirio bod y Data Personol wedi ei gasglu gan y trydydd parti yn unol â'r gyfraith ac ar sail gyfreithlon sy'n ystyried ein gwaith Prosesu arfaethedig o'r Data Personol hwnnw.

5. CYFYNGIAD AR DDIBEN

Mae'n rhaid i Ddata Personol gael ei gasglu at ddibenion penodol, pendant a chyfreithlon yn unig. Ni ddylid ei brosesu ymhellach mewn modd nad yw'n cyd-fynd â'r dibenion hyn.

Ni allwch ddefnyddio Data Personol at ddibenion newydd, gwahanol neu anghydnaws i'r diben y datgelwyd ef pan ddaeth i law yn gyntaf, oni bai eich bod wedi hysbysu'r Testun Data o'r dibenion newydd a bod sail gyfreithlon dros wneud hynny.

6. LLEIHAU DATA

Mae'n rhaid i Ddata Personol fod yn ddigonol, yn berthnasol ac wedi ei gyfyngu i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y mae wedi ei brosesu.

Gallwch ddim ond casglu Data Personol sydd ei angen arnoch ar gyfer eich dyletswyddau: ni ddylech gasglu gormod o ddata. Dylech sicrhau bod unrhyw Ddata Personol a gesglir yn ddigonol ac yn berthnasol i'r dibenion a fwriadwyd.

7. CYWIRDEB

Mae'n rhaid i Ddata Personol fod yn gywir a, lle y bo angen, gael ei gadw'n gyfredol. Mae'n rhaid ei gywiro neu ei ddileu ar unwaith pan fydd yn anghywir.

Dylech sicrhau bod y Data Personol rydym yn ei ddefnyddio ac yn ei ddal yn gywir, yn gyflawn, yn cael ei gadw'n gyfredol ac yn berthnasol i'r diben y casglwyd ef gennym. Dylech wirio cywirdeb unrhyw Ddata Personol pan gesglir ef ac ar gyfnodau rheolaidd ar ôl hyn. Mae'n rhaid i chi gymryd pob cam rhesymol i ddiwygio Data Personol anghywir neu wedi ei ddyddio.

8. CADW

Ni ddylid cadw Data Personol ar ffurf adnabyddadwy am hirach nag sydd ei angen at y dibenion y mae'r data yn cael ei brosesu. Byddwn yn cynnal polisiau a gweithdrefnau cadw er mwyn sicrhau bod Data Personol yn cael ei ddileu yn unol â'r gofyniad hwn.

9. DIOGELWCH

Mae'n rhaid i Ddata Personol gael ei ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon, ac yn erbyn colled, distryw neu ddifrod damweiniol gan fesurau technegol a sefydliadol priodol.

Chi sy'n gyfrifol am ddiogelu'r Data Personol sydd gennym.

Gallwch ddim ond Broesu Data Personol pan fydd yn ofynnol i chi wneud hynny fel rhan o'ch rôl. Ni allwch Broesu Data Personol am unrhyw reswm nad yw'n berthnasol i'ch rôl.

Mae'n rhaid i chi sicrhau eich bod yn dilyn yr holl ganllawiau a gyhoeddir i chi sydd wedi eu dylunio i ddiogelu rhag prosesu Data Personol mewn modd anghyfreithlon neu anawdurdodedig a rhag colli, neu ddifrodi Data Personol yn ddamweiniol. Mae'n rhaid i chi roi sylw penodol i ddiogelu Data Personol Categori Arbennig rhag colled a mynediad, defnydd neu ddatgeliad anawdurdodedig.

10. ADRODD ACHOS O DORRI DATA

Mae'r gyfraith yn gofyn i Reolyddion Data adrodd unrhyw achos o Dorri Data Personol i Swyddfa'r Comisiynydd Gwybodaeth (ICO) ac, mewn achosion penodol, y Testun Data.

Os ydych yn gwybod neu'n amau bod achos o Dorri Data Personol wedi digwydd, peidiwch â cheisio ymchwilio i'r mater eich hun. Dylech ddilyn y polisi adrodd achos o Dorri Data Personol yn Atodiad 1.

11. CYFYNGU TROSGLWYDDO

Mae'r gyfraith yn gosod cyfyngiadau ar drosglwyddo data i wledydd y tu allan i'r Ardal Economaidd Ewropeaidd (EEA) lle nad oes ganddynt gyfreithiau diogelu data digonol. Os oes angen i chi anfon Data Personol y tu allan i'r EEA, dylech gysylltu â'r Swyddog Diogelu Data am gyngor.

12. HAWLIAU'R TESTUN DATA

Mae gan Destunau Data hawliau pan ddaw hi i sut rydym yn trafod eu Data Personol. Mae'r rhain yn cynnwys hawliau o ran y canlynol:

- pan fydd y prosesu yn seiliedig ar ganiatâd cyfreithlon, i dynnu eu caniatâd i brosesu yn ôl ar unrhyw adeg
- derbyn gwybodaeth benodol am ein gweithgareddau prosesu
- cael mynediad at y Data Personol sydd gennym amdanynt
- ein hatal rhag defnyddio eu Data Personol at ddibenion marchnata uniongyrchol
- gofyn i ni ddileu Data Personol os nad yw'n angenrheidiol mwyach i'r dibenion y cafodd ei gasglu neu ei brosesu neu i gywiro data anghywir neu gwblhau data anghyflawn
- cyfyngu prosesu mewn amgylchiadau penodol
- herio prosesu sydd wedi ei gyfiawnhau ar sail ein buddiannau cyfreithlon neu er budd y cyhoedd
- cael eu hysbysu o achos o dorri Data Personol sy'n debygol o arwain at risg uchel i'w hawliau a'u rhyddidau; ac
- mewn rhai amgylchiadau, derbyn neu ofyn i'w Data Personol gael ei drosglwyddo i drydydd parti ar fformat strwythuredig a ddefnyddir yn aml ac y gellir ei ddarllen gan beiriant.

Mae'n rhaid i chi anfon unrhyw gais y byddwch chi'n ei gael gan Destun Data at y Swyddog Diogelu Data.

13. RHANNU DATA

Gallwch ddim ond trosglwyddo Data Personol i ddarparwyr gwasanaethau trydydd parti sy'n cytuno i gydymffurfio â'n polisïau a'n gweithdrefnau ac sy'n cytuno i roi mesurau diogelu digonol ar waith, yn ôl y gofyn. Mae'n rhaid i ni gael cytundeb prosesu data ysgrifenedig yn ei le gydag unrhyw ddarparwyr gwasanaethau o'r fath rydym yn eu defnyddio.

Ynghyd â hyn, er nad yw'n ofyniad cyfreithiol, mae'n arfer da i gael cytundeb rhannu data gydag unrhyw bartneriaid rydym yn gweithio gyda nhw sy'n ymdrin â rhannu Data Personol. Mae'n hanfodol bod gennych sail gyfreithlon eglur dros rannu Data Personol â phartneriaid o'r fath ac eich bod yn trosglwyddo'r Data Personol yn ddiogel.

14. DANGOS CYDYMFFURFIAETH

Mae'r gyfraith yn gofyn i ni gadw cofnodion llawn a chywir o'n holl weithgareddau prosesu. Dylech sicrhau bod unrhyw brosesu rydych yn ei wneud o Ddata Personol cael ei gynnwys yn y cofnodion drwy wirio gyda'r Swyddog Diogelu Data.

Mae gofyniad arnom i sicrhau bod yr holl bobl sy'n gweithio i ni wedi cael hyfforddiant digonol i'w galluogi i gydymffurfio â chyfreithiau preifatrwydd data.

Mae gofyniad arnom i roi mesurau Preifatrwydd trwy Ddyluniad ar waith wrth brosesu Data Personol drwy roi mesurau technegol a sefydliadol priodol ar waith (fel defnyddio ffugenwau) mewn modd effeithiol, er mwyn sicrhau cydymffurfiaeth ag egwyddorion preifatrwydd data.

Mae'n rhaid i reolyddion data hefyd gynnal Aseidiadau o'r Effaith ar Breifatrwydd Data (DPIAs) mewn perthynas â phrosesu risg uchel. Os ydych yn credu bod y prosesu rydych yn ei wneud yn risg uchel, siaradwch â'r Swyddog Diogelu Data.

Mae'n rhaid i ni hefyd brofi ein systemau a'n prosesau'n rheolaidd i asesu cydymffurfiaeth. Mae'n rhaid i chi adolygu'r holl systemau a phrosesau sydd o dan eich rheolaeth yn rheolaidd er mwyn sicrhau eu bod yn cydymffurfio â'r polisi hwn a gwirio bod mesurau llywodraethu

ac adnoddau digonol ar waith i sicrhau bod Data Personol yn cael ei ddefnyddio a'i ddiogelu'n briodol.

ADOLYGU

Mawrth 2022 (Dyddiad adolygu: Mawrth 2024)

CGGC – Prif Swyddfa
Un Rhodfa'r Gamlas
Heol Dumballs
Caerdydd
CF10 5BF
Ffôn: 0300 111 0124
E-bost: help@wcva.cymru

www.wcva.cymru

Elusen Gofrestredig 218093 | Cwmni Cyfyngedig drwy Warant 425299 |
Cofrestrwyd yng Nghymru

ADRODD ACHOS O DORRI DATA

Mae GDPR y DU yn gosod dyletswydd ar fudiadau i adrodd mathau penodol o doriadau data personol i'r awdurdod goruchwyllo perthnasol (yr ICO). Mae'n rhaid gwneud hyn o fewn 72 awr i ddod yn ymwybodol o'r toriad, lle y bo'n ymarferol. Os yw'r toriad yn debygol o arwain at risg uchel o effeithio'n niweidiol ar hawliau a rhyddidau unigolion, mae'n rhaid hysbysu'r unigolion cyn gynted â phosibl.

Swyddog Diogelu Data (DPO) CGGC yw'r unig un a all wneud y penderfyniad i adrodd toriad data, naill ai i Swyddfa'r Comisiynydd Gwybodaeth (ICO) neu i'r testunau data eu hunain.

Mae dyletswydd ar bob aelod staff i adrodd achosion o dorri data i'r Swyddog Diogelu Data cyn gynted ag y bydd yn dod yn ymwybodol o'r toriad neu, os nad yw'r Swyddog Diogelu Data yn bresennol, dylid adrodd y toriad i'r Prif Swyddog Gweithredol. Diffinnir ymwybyddiaeth fel pan fydd aelod staff yn weddol ffyddiog bod digwyddiad diogelwch wedi digwydd a bod hyn wedi arwain at roi data personol mewn perygl.

Gellir categorio achos o dorri data personol fel a ganlyn:

'*Tor-cyfrinachedd*' – pan fydd data personol yn cael ei ddatgelu heb awdurdod neu'n ddamweiniol neu pan fydd mynediad anawdurdodedig neu ddamweiniol at y data hwn

'*Tor-argaeledd*' – pan gollir mynediad at ddata personol, neu pan fydd y data hwn yn cael ei ddinistrio, yn ddamweiniol neu heb awdurdod

'*Tor-uniondeb*' – pan fydd data personol yn cael ei addasu heb awdurdod neu'n ddamweiniol

Dylid hefyd nodi y gall achos o dorri data, yn dibynnu ar yr amgylchiadau, ymwneud â chyfrinachedd, argaeledd ac uniondeb data personol ar yr un pryd, yn ogystal ag unrhyw gyfuniad o'r rhain.

Isod, ceir rhai enghreifftiau ffug i'ch cynorthwyo i adnabod achosion o dorri data, y broses hysbysu y mae'r Swyddog Diogelu Data yn ei dilyn a gwybodaeth ychwanegol sy'n ymwneud â'r senario a gyflwynir.

ENGHRAIFFT	DPO I HYSBYSU'R AWDURDOD GORUCHWYLIO (ICO)?	DPO I HYSBYSU'R TESTUN DATA?	SYLWADAU
Mae data personol ar gof bach USB wedi'i amgryptio. Mae'r cof bach USB yn cael ei ddwyn mewn lladrad.	Na	Na	Cyhyd â bod y data wedi'i amgryptio gydag 'algorithm modern' (hynny yw, amgryptio i safonau AES256 ar gyfer darparu gwybodaeth personol) ac nad yw'r allwedd unigryw dan fygythiad, nid yw hwn yn doriad sydd angen ei adrodd.
Mae data personol yn cael ei dynnu o wefan ddiogel a reolir gan CGGC yn ystod ymosodiad seiber.	Ie. Bydd y DPO yn adrodd i'r ICO ac yn nodi a oes unrhyw ganlyniadau posibl i unigolion.	Ie. Bydd y DPO yn hysbysu unigolion yn dibynnu ar natur y data personol sydd wedi ei effeithio a'r canlyniadau posibl iddynt.	Hyd yn oed os nad ystyrir bod y risg yn 'uchel' i unigolion, gall y DPO ddewis hysbysu testunau data'r toriad o hyd, oherwydd gall y datgeliad cychwynnol hwn arwain at dor-cyfrinachedd ychwanegol mewn manau eraill.
Ceir ymosodiad meddalwedd wystlo, ac mae hyn yn peri i ddata gael ei amgryptio. Nid oes copïau wrth gefn ar gael, ac ni ellir adfer y data. Ar ôl ymchwiliad, daw i'r amlwg mai dim ond amgryptio a ddigwyddodd ac nad oedd unrhyw faleiswedd arall yn bresennol .	Ie	Ie. Dim ond yr unigolion a effeithiwyd arnynt sydd angen eu hysbysu pan fydd cadarnhad positif, clir nad yw pobl eraill wedi eu heffeithio.	Pe bai copïau wrth gefn ar gael a gallai'r data gael ei adfer mewn da bryd, ni fyddai angen adrodd hwn, gan na fyddai'n golled barhaol. Ond, fe allai'r ICO ystyried ymchwiliad i asesu'r gydymffurfiaeth yn fwy cyffredinol. Fodd bynnag, dylai'r tîm diogelu data ei gofnodi fel digwyddiad ar gofnodion canolog y grŵp.
Mae unigolyn wedi derbyn cyfathrebiad gan CGGC sy'n cynnwys data personol rhywun arall. O fewn yr ymchwiliad 24 awr cychwynnol, ymddengys fod toriad data personol wedi digwydd a gallai unigolion eraill fod wedi eu heffeithio.	Ie	Ie. Dim ond yr unigolion a effeithiwyd arnynt sydd angen eu hysbysu pan fydd cadarnhad positif, clir nad yw pobl eraill wedi eu heffeithio.	Os canfyddir, ar ôl ymchwilio ymhellach, fod mwy o unigolion wedi eu heffeithio, yna bydd y DPO yn diweddarau'r ICO yn unol â hynny. Mewn amgylchiadau arbennig, mae'n bosibl y bydd yn rhaid i'r DPO hysbysu unigolion eraill os yw'r lefel o risg iddynt hwy wedi cynyddu yn dilyn yr ymchwiliad.
Mae ymosodiad seiber yn digwydd, a chaiff enwau defnyddwyr, cyfrineiriau a manylion personol eraill eu cyhoeddi ar-lein gan yr ymosodwr.	Ie	Ie. Diffinnir hyn fel risg uchel i'r unigolion eu hunain.	Dylid mynnu bod cyfrineiriau yn cael eu hailosod ar y cyfrifon a effeithiwyd, ac ystyried ehangu hyn i'r holl ddefnyddwyr os pennir fod y risg yn bosibl. Bydd yn rhaid cymryd camau eraill i leihau'r risg i'r unigolion a effeithir lle bynnag y bo'n bosibl.

ENGHRAIFFT	DPO I HYSBYSU'R AWDURDOD GORUCHWYLIO (ICO)?	DPO I HYSBYSU'R TESTUN DATA?	SYLWADAU
Mae cwmni cynnal gwefan ar gyfer y grŵp yn darganfod gwall yn y cod sy'n rheoli'r broses o ddilysu defnyddwyr. O ganlyniad, gall unrhyw ddefnyddiwr gael mynediad at unrhyw fanylion cyfrif.	Ie. Mae'n rhaid i'r cwmni cynnal gwefan hysbysu ei gleientiaid sydd wedi eu heffeithio cyn gynted â phosibl. Mae'n rhaid i'r cwmni gwefan hysbysu'r grŵp o'r tor-data a'r camau sydd eisoes wedi eu cymryd. Ar ôl hyn, cyfrifoldeb y grŵp yw hysbysu'r ICO o'r tor-data.	Ie. Dylai'r cwmni sy'n cynnal y wefan (lle y bo'n berthnasol) a'r grŵp eu hunain wneud hyn, pan bennir fod y risg yn uchel.	Yn yr achos hwn, y cwmni sy'n cynnal y wefan yw prosesydd y grŵp (fel rheolydd). Mae ganddynt gyfrifoldeb i'r testun data i'w hysbysu o'r tor-data, a byddai'r cyfrifoldeb hwn eisoes wedi ei nodi iddynt yn y cytundeb prosesu data trydydd parti gyda'r grŵp. Mae gan y grŵp hefyd gyfrifoldeb i hysbysu'r unigolion, oherwydd gallai niweidio eu henw da.
Mae data personol 5,000 o staff yn cael ei anfon i'r rhestr bostio anghywir sydd ag 1,000+ o dderbynyddion.		Ie. Bydd y DPO yn hysbysu unigolion, yn dibynnu ar y cwmpas a'r math o ddata personol sydd o dan sylw a difrifoldeb canlyniadau posibl.	Byddai hyn yn cael ei ystyried yn driniaeth ddiogel o ddata; byddai angen gwneud pob ymdrech i liniaru risgiau pellach i hawliau a rhyddidau'r testunau data eu hunain.
Mae e-bost marchnata uniongyrchol yn cael ei anfon at dderbynyddion yn y maes 'i' ('to') yn hytrach na'r maes 'bcc', ac felly'n galluogi pob derbynnydd i weld cyfeiriad e-bost y derbynyddion eraill.	Ie. Efallai y bydd angen camau gweithredu pellach os oes nifer mawr o destunau data wedi eu heffeithio, categorïau arbennig o ddata wedi eu datgelu neu os oes risg uchel arall wedi ei nodi, e.e. enwau defnyddwyr a chyfrineiriau.	Ie. Bydd y DPO yn hysbysu unigolion, yn dibynnu ar y cwmpas a'r math o ddata personol sydd o dan sylw a difrifoldeb canlyniadau posibl.	Mewn amgylchiadau arbennig, efallai na fydd angen hysbysu'r testunau data, e.e. os nad oes categorïau arbennig o ddata wedi eu datgelu neu os yw'r niferoedd a effeithiwyd yn parhau i fod yn isel. Mae'n bosibl y bydd amgylchiadau yn newid wrth i'r ymchwiliad fynd yn ei flaen, ac efallai y bydd hefyd angen ailedrych ar yr opsiwn o hysbysu'r testunau data yn ddiweddarach yn ystod yr ymchwiliad.