

|  |
| --- |
| **Tai Gogledd Cymru** |
| **Polisi Diogelu Data GDPR** |

|  |  |
| --- | --- |
| **Perchennog** | Malcolm Wilson |
| **Cyfarwyddiaeth** | Adnoddau – TG |
| **Cymeradwywyd gan** | Y Bwrdd 29 Mawrth 2018 |
| **Dyddiad adolygu nesaf** | Mawrth 2020 |
|  |  |

|  |  |  |
| --- | --- | --- |
|  | **Cynnwys** | **Tudalen** |
| **1** | Cyflwyniad | 2 |
| **2** | Cwmpas ac amcanion polisi | 2 |
| **3** | Egwyddorion diogelu data | 4 |
| **4** | Hawliau Gwrthrychau Data | 8 |
| **5** | Cydsyniad | 9 |
| **6** | Cyfrifoldebau o dan Y Rheoliad Cyffredinol ar Ddiogelu Data | 10 |
| **7** | Hysbysu | 11 |
| **8** | Datgelu data | 12 |
| **9** | Marchnata uniongyrchol | 13 |
| **10** | Cyflogeion | 14 |
| **11** | Cyflenwyr a Chontractwyr | 15 |
| **12** | Asesiad o’r Effaith ar Risg a Diogelu Data | 15 |
| **13** | Torri diogelwch | 16 |
| **14** | Cofnodion a Chynnal a Chadw | 16 |
| **15** | Hyfforddiant | 17 |
| **16** | Monitro ac adrodd | 17 |
| **17** | Polisïau cysylltiedig | 18 |
|  | **Atodiad A – Rhestr o Ddiffiniadau** | 19 |

**Mae Tai Gogledd Cymru yn ymrwymedig i gydraddoldeb ac amrywiaeth. Mae’r polisi hwn wedi ystyried Deddf Cydraddoldeb 2010 a’i nodweddion gwarchodedig, sef: hil, rhyw, ailbennu rhywedd, anabledd, crefydd neu gred, cyfeiriadedd rhywiol, oedran, priodas, priodas sifil a phartneriaeth sifil, a beichiogrwydd a mamolaeth yn benodol.**

**Byddwn yn gwneud yn siŵr bod ein holl ddulliau cyfathrebu yn gwbl hygyrch ac i gyflawni hyn, os bydd angen i bolisi neu ddogfen fod ar gael mewn fformatau eraill, byddwn yn eu darparu.**

**1. Cyflwyniad**

1.1 Bydd y Rheoliad Cyffredinol ar Ddiogelu Data (GDPR) 2016 yn weithredol o 25 Mai 2018 ac mae’n disodli’n llwyr yr holl gyfreithiau Diogelu Data blaenorol. Ei ddiben yw diogelu ‘hawliau a rhyddid’ unigolion byw, ac i sicrhau nad yw data personol yn cael ei brosesu heb yn wybod iddynt a’i fod yn cael ei brosesu gyda’u cydsyniad hwy.

1.2 Mae’r GDPR yn cyflwyno nifer o gysyniadau newydd a gwelliannau i hawliau gwrthrychau data. Ceir crynodeb o’r rheoliadau newydd isod:

* sicrhau cydsyniad penodol gan wrthrychau data i ddefnyddio eu data personol;
* prosesu gwybodaeth bersonol berthnasol a digonol; dim ond pan fydd hyn yn gwbl angenrheidiol at ddibenion sefydliadol cyfreithlon;
* dim ond casglu’r wybodaeth bersonol ofynnol sydd ei hangen at ddibenion hyn a pheidio prosesu gwybodaeth bersonol ormodol;
* darparu gwybodaeth glir i unigolion ynghylch sut y defnyddir eu gwybodaeth bersonol a chan bwy;
* prosesu gwybodaeth bersonol yn deg a chyfreithlon;
* cynnal rhestr o’r categorïau gwybodaeth bersonol y mae Cymdeithas Tai Gogledd Cymru yn eu prosesu;
* mae gwybodaeth bersonol yn gywir a, lle bydd angen, yn gyfredol;
* dim ond cadw gwybodaeth bersonol am gyhyd ag y bydd ei hangen am resymau cyfreithiol neu reoliadol neu, at ddibenion sefydliadol cyfreithlon;
* cadw’r holl wybodaeth bersonol yn ddiogel;
* dim ond trosglwyddo gwybodaeth bersonol y tu allan i’r Undeb Ewropeaidd mewn amgylchiadau lle gellir ei diogelu’n briodol neu pan fydd safonau cyfatebol yn berthnasol;
* cymhwyso’r eithriadau amrywiol a ganiateir;
* y gofyniad i benodi Swyddog Diogelu Data (SDD) mewn rhai amgylchiadau;
* mae ‘categorïau penodol’ o ddata personol (data personol sensitif yn flaenorol) yn cael eu hymestyn i gynnwys data biometreg a genetig;
* proses orfodol o adrodd achosion o dorri/colli data;
* trefniadau diogelwch gwell ar gyfer data personol, e.e. amgryptio ac anhysbysu;
* parchu hawliau mynediad y gwrthrych, gan gynnwys darpariaethau newydd megis hygludedd data;
* sicrhau bod gwrthrychau data, h.y. unigolion yr ydym yn cadw data amdanynt, yn ymwybodol o’u hawliau cyn casglu neu brosesu unrhyw wybodaeth bersonol.

Mae Atodiad A yn darparu rhestr o ddiffiniadau.

**2. Datganiad, cwmpas ac amcanion polisi**

Mae Cymdeithas Tai Gogledd Cymru yn ymrwymedig i gydymffurfio â holl gyfreithiau perthnasol yr UE ac Aelod-wladwriaethau mewn cysylltiad â data personol, a diogelu ‘hawliau a rhyddid’ unigolion y mae CTGC yn casglu ac yn prosesu eu gwybodaeth yn unol â’r GDPR.

Mae CTGC yn defnyddio, o reidrwydd ac fel mater o drefn, gwybodaeth bersonol pan fydd yn cyflawni sawl agwedd o’u busnes o ddydd i ddydd. Mae’r sefydliad cyfan yn ddarostyngedig i’r polisi, gyda rhai gofynion yn dosbarthu ac yn gorfodi cyfrifoldebau ar sefydliadau partner, e.e. ein contractwyr cynnal a chadw. (Fel arfer maent yn Brosesydd Data data personol yr ydym wedi’i gasglu yn ein rôl fel Rheolydd Data).

Y data personol sy’n cael ei gwmpasu gan GDPR yw’r holl ddata yn ein systemau cyfrifiadurol, gan gynnwys ein System Rheoli Tai, System Rheoli Dogfennau, e-bost, dogfennau Word, taenlenni Excel, yn ogystal â systemau strwythuredig ffeiliau â llaw, h.y. papur. (Mae system ffeilio strwythuredig yn cael ei diffinio fel system sydd â math o fynegai, sy’n galluogi mynediad cyflym a rhwydd at y dogfennau unigol ynddi). Ni fyddai system ffeilio sydd mewn trefn dyddiadau yn unig, heb unrhyw fynegai o’r fath, yn cael ei hystyried yn system strwythuredig). Er mwyn osgoi unrhyw amheuaeth, mae cwmpas GDPR hefyd yn cynnwys negeseuon testun, fideos, ffotograffau, nodiadau post-it, llyfrau nodiadau, allbrintiau a llythyrau a ysgrifennwyd â llaw ac yn y blaen.

Mae’r GDPR a’r polisi hwn yn berthnasol i:

* Holl swyddogaethau prosesu data personol CTGC, gan gynnwys y rhai a gyflawnir ar ddata personol cwsmeriaid, cleientiaid, cyflogeion, cyflenwyr a phartneriaid ac unrhyw ddata personol arall y mae’r sefydliad yn ei brosesu o unrhyw ffynhonnell, gan gynnwys data wedi’i archifo, yn ddigidol ac ar bapur.
* Holl gyflogeion CTGC. Ymdrinnir ag unrhyw achos o dorri’r GPDR (neu’r polisi hwn) yn unol â’r polisi disgyblu a gallai hefyd fod yn drosedd, ac os felly bydd yr awdurdodau priodol yn cael eu hysbysu ynghylch y mater cyn gynted â phosibl.

Mae Swyddog Diogelu Data (SDD) yn y broses o gael ei benodi. Mae’r SDD yn gyfrifol am adolygu’r gofrestr brosesu yn achos unrhyw newidiadau i weithgareddau CTGC, adolygu dulliau rheoli neu unrhyw ofynion ychwanegol a nodwyd drwy Asesiadau o Effaith Diogelu Data. Efallai y bydd angen i ddogfennaeth o’r fath fod ar gael i’r awdurdod goruchwylio, ar gais.

Disgwylir i bartneriaid ac unrhyw drydydd parti sy’n gweithio gyda CTGC, sydd â mynediad at ddata personol, fod wedi darllen, deall a chydymffurfio â’r gofynion a’r cytundebau yn ein polisi Cyfrifoldebau Diogelu Data Cyflenwyr. Mae’r polisi hwn yn gosod rhwymedigaethau ar y trydydd parti nad ydynt yn llai rhwymedigaethus na’r rhai y mae CTGC wedi ymrwymo iddynt, ac mae’n rhoi’r hawl i archwilio cydymffurfiaeth gyda’r cytundeb Cyflenwyr.

Amcanion y polisi yw:

* diogelu buddiannau data personol unigolion a rhanddeiliaid allweddol eraill drwy ddefnyddio gweithdrefnau a rheolaethau priodol.
* darparu’r fframwaith ategol ar gyfer cyflawni a chynnal cydymffurfiaeth GDPR.
* sicrhau bod CTGC yn cyflawni dyletswyddau statudol, rheoleiddiol, cytundebol a/neu broffesiynol perthnasol.

**3. Egwyddorion diogelu data**

**3.1. Mae’n rhaid diogelu data yn gyfreithlon, teg a thryloyw.**

*Cyfreithlon*

Mae’n rhaid nodi sail gyfreithlon cyn prosesu data personol. Cyfeirir at hyn yn aml at yr ‘amodau ar gyfer prosesu’, e.e. cydsyniad.

*Teg*

Er mwyn sicrhau bod prosesu yn deg, mae’n rhaid i’r Rheolydd Data sicrhau bod gwybodaeth benodol ar gael i wrthrychau’r data, os yw’n ymarferol. Mae hyn yn berthnasol p’un a gasglwyd y data personol yn uniongyrchol gan wrthrychau’r data neu o ffynonellau eraill.

Mae gan y GDPR ofynion cynyddol am y wybodaeth a ddylai fod ar gael i wrthrychau data, sy’n cael eu cwmpasu yn y gofyniad ‘Tryloywder’.

*Tryloyw*

Mae’r GDPR yn cynnwys rheolau ar roi gwybodaeth ar breifatrwydd i wrthrychau data, a nodir yn Erthyglau 12, 13 ac 14 y rheoliadau. Mae’r rhain yn fanwl a phenodol, ac yn rhoi pwyslais ar sicrhau bod hysbysiadau preifatrwydd yn hawdd eu deall a hygyrch. Mae’n rhaid cyfleu gwybodaeth i wrthrych y data mewn ffurf ddealladwy gan ddefnyddio iaith glir a hawdd ei deall. (Gweler polisi Preifatrwydd Cwsmeriaid a Hysbysiad Prosesu Teg CTGC).

Mae’n rhaid i wybodaeth benodol i’w darparu i wrthrych y data, fel isafswm, gynnwys:

* hunaniaeth a manylion cyswllt y rheolydd a chynrychiolydd y rheolydd, os o gwbl;
* manylion cyswllt y Swyddog Diogelu Data;
* dibenion y prosesu y bwriedir y data personol ar ei gyfer yn ogystal â’r sail gyfreithlon dros y prosesu;
* y cyfnod y bydd y data personol yn cael ei storio;
* bodolaeth hawliau i ofyn am fynediad, cywiro, diddymu neu wrthwynebu’r prosesu, a’r amodau (neu ddiffyg amodau) sy’n gysylltiedig ag arfer yr hawliau hynny, er enghraifft a effeithir ar gyfreithlondeb prosesu blaenorol;
* categorïau’r data personol dan sylw;
* derbynwyr neu gategorïau o dderbynwyr y data personol, lle y bo’n berthnasol;
* pan fo’n berthnasol, bod y rheolydd yn bwriadu trosglwyddo data personol i dderbynnydd mewn trydedd wlad a lefel y diogelwch a roddir i’r data;
* unrhyw wybodaeth bellach angenrheidiol i warantu prosesu teg.

**3.2. Dim ond at ddibenion penodol a chyfreithlon y gellir casglu data personol**

Ni ddylid defnyddio data a gasglwyd at ddibenion penodol at ddiben sy’n wahanol i’r rhai yr hysbyswyd yr awdurdod goruchwylio yn eu cylch, fel rhan o gofrestriad GDPR CTGC. Cyfeirnod cofrestru CTGC yw Z5865343 a gellir gweld manylion cofnod cofrestru ar wefan yr awdurdod goruchwylio <https://ico.org.uk/ESDWebPages/Entry/Z5865343>

Pan fydd newid i ddiben (ac eithrio’r diben gwreiddiol y casglwyd y data ar ei gyfer), cyn prosesu pellach, mae’n rhaid i ni ddarparu’r wybodaeth ar y diben newydd i wrthrych y data.

**3.3. Mae’n rhaid i ddata personol fod yn ddigonol, perthnasol ac wedi’i gyfyngu i’r diben angenrheidiol ar gyfer prosesu.**

Y SDD sy’n gyfrifol am sicrhau nad yw CTGC yn casglu gwybodaeth nad yw’n gwbl angenrheidiol at y diben y cafodd ei chasglu.

Mae’n rhaid i bob ffurflen casglu data (electronig neu bapur), gynnwys gofynion casglu data mewn systemau gwybodaeth newydd, gynnwys datganiad prosesu teg neu ddolen i ddatganiad preifatrwydd a’i gymeradwyo gan y SDD.

Bydd y SDD yn sicrhau bod dulliau casglu data yn cael eu harchwilio’n rheolaidd, i sicrhau bod data a gasglwyd yn parhau i fod yn ddigonol, perthnasol ac nad yw’n ormodol.

Os rhoddir neu cesglir data sy’n ormodol neu nad oes ei angen yn benodol gan weithdrefnau cyhoeddedig CTGC, y SDD sy’n gyfrifol am sicrhau ei fod yn cael ei ddileu neu ei ddinistrio’n ddiogel yn unol â’r polisi Cadw Dogfennau a Data.

**3.4. Mae’n rhaid i ddata personol fod yn gywir a chyfredol.**

Mae’n rhaid i ddata sy’n cael ei gadw am gyfnod hir gael ei adolygu a’i ddiweddaru yn ôl yr angen. Ni ddylid cadw unrhyw ddata oni fydd yn rhesymol tybio ei fod yn gywir. Bydd cwblhau ffurflen gofrestru neu ffurflen gais briodol yn arwydd bod y data a gynhwysir ynddi yn gywir ar ddyddiad ei chyflwyno.

Er y dylai ein cwsmeriaid a’n staff ein hysbysu ynghylch unrhyw newidiadau i amgylchiadau, bydd angen ymgyrchoedd casglu a gwirio rhagweithiol, rheolaidd. CTGC sy’n gyfrifol am sicrhau bod unrhyw hysbysiad o newid mewn amgylchiadau yn cael ei nodi a’i weithredu.

Y SDD sy’n gyfrifol am sicrhau:

* Bod dyddiadau cadw’r holl ddata personol sy’n cael ei brosesu gan CTGC yn cael eu hadolygu, o leiaf yn flynyddol, er mwyn nodi unrhyw ddata nad oes ei angen mwyach a threfnu i’w ddileu/dinistrio’n ddiogel.
* Ein bod yn ymateb i geisiadau i gywiro gan wrthrychau data o fewn un mis. Os bydd CTGC yn penderfynu na fydd yn cydymffurfio â’r cais, mae’n rhaid i’r SDD ymateb i wrthrych y data i esbonio’r rheswm dros hyn a’u hysbysu o’u hawl i wneud cwyn.
* Ein bod yn gwneud trefniadau priodol pan allai sefydliadau trydydd parti fod wedi trosglwyddo data personol anghywir neu anghyfredol, i’w hysbysu na ddylid defnyddio’r wybodaeth i hysbysu penderfyniadau am yr unigolion dan sylw ac am drosglwyddo unrhyw gywiriadau.

**3.5. Mae’n rhaid cadw data ar ffurf lle gellir adnabod gwrthrych y data, dim ond am gyhyd ag y bydd angen ar gyfer prosesu.**

Pan gedwir data personol y tu hwnt i’r data prosesu, dylid ei ‘gymylu’ drwy ei leihau, ei amgryptio neu ddefnyddio ffugenwau, er mwyn diogelu hunaniaeth gwrthrych y data. Mae hyn yn ddibynnol ar y galluoedd technegol sydd ar gael.

Cedwir data personol yn unol â’n polisi Cadw Dogfennau a Data. Ar ôl i’r dyddiad cadw fynd heibio, mae’n rhaid ei ddinistrio’n ddiogel.

Mae’n rhaid i’r SDD gymeradwyo’n benodol unrhyw achos o gadw data sy’n mynd y tu hwnt i’r cyfnodau cadw a sicrhau bod y cyfiawnhad dros hynny wedi’i nodi yn unol â deddfwriaeth diogelu data.

**3.6. Mae’n rhaid prosesu data mewn dull sy’n sicrhau’r diogelwch priodol.**

Bydd y SDD yn cynnal asesiad risg, a fydd yn ystyried holl amgylchiadau gweithrediadau rheoli neu brosesu CTGC.

Wrth benderfynu ar briodoldeb, bydd y SDD hefyd yn ystyried graddau’r niwed neu golled bosibl y gellir ei achosi i unigolion pe byddai achos o dorri diogelwch yn digwydd; effaith unrhyw achos o dorri diogelwch ar CTGC; ac unrhyw niwed tebygol i enw da, gan gynnwys y posibilrwydd o golli ymddiriedaeth cwsmeriaid.

Wrth asesu mesurau technegol priodol, bydd y SDD yn ystyried y canlynol:

* Diogelu cyfrineiriau;
* Cloi terfynellau segur yn awtomatig;
* Cael gwared ar hawliau mynediad ar gyfer USB a chyfryngau cof eraill;
* Meddalwedd gwirio am firysau a waliau tân;
* Hawliau mynediad ar sail hawliau gan gynnwys y rhai sy’n cael eu haseinio i staff dros dro;
* Amgryptio dyfeisiau sy’n gadael lleoliad sefydliadau, er enghraifft gliniaduron;
* Diogelu rhwydweithiau lleol ac ardal eang;
* Technolegau gwella preifatrwydd er enghraifft defnyddio ffugenwau a dulliau anhysbysu.
* Nodi safonau diogelwch rhyngwladol priodol sy’n berthnasol i CTGC.

Wrth asesu mesurau sefydliadol priodol, bydd y SDD yn ystyried y canlynol:

* Y lefelau hyfforddiant priodol drwy CTGC;
* Mesurau sy’n ystyried dibynadwyedd cyflogeion;
* Cynnwys diogelu data mewn contractau cyflogaeth;
* Nodi mesurau camau disgyblu ar gyfer achosion o dorri data;
* Monitro staff am gydymffurfiaeth gyda safonau diogelwch perthnasol;
* Rheolaethau mynediad ffisegol i gofnodion electronig a phapur;
* Mabwysiadu polisi desg clir;
* Storio data papur mewn cypyrddau gwrth-dân;
* Rheolaethau priodol ar ddyfeisiau electronig cludadwy y tu allan i’r gweithle;
* Rheolaethau a gwiriadau priodol ar y defnydd o ddyfeisiau personol y cyflogai ei hun sy’n cael eu defnyddio yn y gweithle (ar hyn o bryd nid oes unrhyw drefniadau ar waith ar gyfer dod â’ch dyfeisiau eich hun);
* Mabwysiadu rheolau clir ar gyfrineiriau;
* Creu copïau wrth gefn rheolaidd o ddata personol a storio’r cyfryngau oddi ar y safle.

Dewiswyd y rheolaethau hyn ar y sail o risgiau a nodwyd i ddata personol a’r posibilrwydd o greu niwed neu ofid i unigolion y mae eu data’n cael ei brosesu.

Ni ddylid trosglwyddo data personol i wlad neu diriogaeth y tu allan i’r Undeb Ewropeaidd oni bai bod ganddynt lefel ddigonol o ddiogelwch ar gyfer ‘hawliau a rhyddid’ gwrthrychau data.

Mae’r GDPR yn cynnwys cryn fanylder ar y rheolaethau y mae’n rhaid iddynt fod yn weithredol ar gyfer trosglwyddo data y tu allan i ardal yr Undeb Ewropeaidd ac mae nifer o gysyniadau’n cael eu cyflwyno. Rhoddir disgrifiad byr o drefniadau a dulliau diogelu yn y weithdrefn ar wahân - Trosglwyddo data personol y tu allan i ardal yr UE.

**4. Hawliau gwrthrychau data**

**4.1 Prosesu Data**

Mae gan wrthrychau data yr hawliau canlynol mewn cysylltiad â phrosesu data a’r data a gofnodir amdanynt:

* Gwneud ceisiadau mynediad pwnc ynglŷn â natur gwybodaeth a gedwir ac i bwy y cafodd ei datgelu. Mae nifer o eithriadau yn berthnasol pan na fydd rhaid datgelu data personol - gweler y weithdrefn Cais Mynediad Pwnc.
* Atal prosesu at ddibenion marchnata uniongyrchol.
* Cael gwybod am fecaneg proses awtomataidd o wneud penderfyniadau a fydd yn cael effaith arwyddocaol arnynt.
* Sicrhau na wneir unrhyw benderfyniadau arwyddocaol a fydd yn effeithio arnynt gan brosesau awtomataidd yn unig.
* Erlyn am iawndal os byddant yn dioddef unrhyw niwed o ganlyniad i unrhyw achos o fynd yn groes i’r GDPR.
* Cymryd camau i unioni, gwahardd, dileu neu ddinistrio data anghywir, gan gynnwys yr hawl i gael eich anghofio.
* Gofyn i’r awdurdod goruchwyliol asesu a fu achos o fynd yn groes i unrhyw rai o ddarpariaethau’r GDPR.
* Cael data personol wedi’i ddarparu iddynt mewn fformat strwythuredig, a ddefnyddir yn gyffredin ac y gellir ei ddarllen gan beiriannau, a chael yr hawl i’r data hwnnw gael ei drosglwyddo i reolydd arall.
* Gwrthwynebu i unrhyw broffilio awtomataidd sy’n digwydd heb gydsyniad.
* Pan fydd yn bosibl, atal prosesu data pan fydd ymholiad yn ei gylch neu pan fydd yn destun Cais Mynediad Pwnc.

**4.2 Cwynion**

Gall gwrthrychau data sy’n dymuno cwyno ynglŷn â’r ffordd y cafodd eu gwybodaeth bersonol ei phrosesu:

* defnyddio’r weithdrefn gwyno;
* cwyno’n uniongyrchol i’r SDD;
* cwyno i’r awdurdod goruchwylio.

**4.3 Hawliau mynediad at ddata**

Mae gan wrthrychau data yr hawl i gael mynediad at unrhyw ddata personol a gedwir gan CTGC mewn fformat electronig a chofnodion llaw sy’n ffurfio rhan o system ffeilio strwythuredig. Mae hyn yn cynnwys yr hawl i archwilio cyfeiriadau personol cyfrinachol a dderbyniwyd gan CTGC a gwybodaeth a dderbyniwyd gan sefydliadau trydydd parti am y person hwnnw.

Ymdrinnir â Cheisiadau Mynediad Pwnc fel y disgrifir yn y Weithdrefn Cais Mynediad Pwnc Diogelu Data.

**5. Cydsyniad**

Mae CTGC yn deall mai ystyr ‘cydsyniad’ yw:

* fe’i rhoddwyd yn benodol ac yn glir, a’i fod yn arwydd penodol, gwybodus a diamwys o ddymuniadau gwrthrych y data, trwy ddatganiad neu weithred gadarnhaol glir, yn dynodi cytundeb i brosesu data personol sy’n gysylltiedig ag ef neu hi. Gall gwrthrych y data dynnu eu cydsyniad yn ôl unrhyw amser.
* mae gwrthrych y data wedi’i hysbysu’n llwyr ynglŷn â’r prosesu arfaethedig ac mae wedi dynodi eu cytundeb, tra mewn cyflwr addas i wneud hynny a heb i unrhyw un roi pwysau arnynt. Ni fydd cydsyniad a sicrhawyd o dan orfodaeth neu ar sail gwybodaeth gamarweiniol yn sail ddilys ar gyfer prosesu.

Bydd tynnu cydsyniad yn ôl yn effeithio ar sut, neu’n wir a allwn, ddarparu gwasanaethau i’r cwsmeriaid hynny. Bydd angen newid y meysydd data mewn systemau priodol i ddynodi ‘gwrthodwyd’.

Mae’n rhaid bod rhywfaint o gyfathrebu gweithredol rhwng y partïon i ddangos cydsyniad gweithredol. Ni ellir tybio cydsyniad oherwydd diffyg ymateb i gyfathrebiad. Mae’n rhaid i’r Rheolydd allu arddangos y sicrhawyd cydsyniad ar gyfer y gweithrediad prosesu.

Ar gyfer data sensitif, mae’n rhaid sicrhau cydsyniad ysgrifenedig penodol gwrthrychau data oni fydd sail gyfreithiol arall yn bodoli ar gyfer prosesu.

Yn y rhan fwyaf o achosion, bydd cydsyniad i brosesu data personol a sensitif yn cael ei sicrhau’n arferol gan CTGC gan ddefnyddio dogfennau cydsyniad safonol, e.e. pan fydd cleient newydd yn llofnodi Cytundeb Tenantiaeth.

Pan fydd CTGC yn darparu gwasanaethau ar-lein i blant (sy’n cael eu diffinio o dan 16 oed, oedran cydsyniad y DU), mae’n rhaid sicrhau awdurdodaeth rhieni neu ofalwr.

Mewn rhai amgylchiadau penodol, gall CTGC dderbyn gwybodaeth am breswylwyr gan asiantaethau partner, yn arbennig yr heddlu neu awdurdodau lleol. Dylai cyflogeion sydd angen cyngor ar sut i drin y wybodaeth hon drafod y mater gyda’u rheolwr neu’r SDD.

Nid yw’r ‘porth’ prosesu cyfreithlon, sef bod angen prosesu at ddibenion buddion cyfreithlon, ar gael yn bendant i awdurdodau cyhoeddus. Mae’n rhaid i unrhyw rwymedigaeth gyfreithlon neu dasg er budd y cyhoedd fod wedi’i gofnodi yng nghyfreithiau’r UE neu Brydain, ac mae’n rhaid i hyn fod o fudd i’r cyhoedd ac yn gymesur â’r nod.

Mae’n debygol na fydd y porth prosesu cyfreithlon ‘cydsyniad a roddir gan y preswylydd’, a ddefnyddiwyd gennym yn hanesyddol, yn cyflawni gofynion mwy llym GDPR. Felly, adolygir pob porth i sicrhau eu bod yn cydymffurfio.

Mae Darparwyr Cofrestredig yn cael eu dosbarthu fel Cymdeithasau Budd Cymunedol ac maent yn sefydliadau ‘hybrid’, hanner ffordd rhwng y sectorau cyhoeddus a phreifat. Yn absenoldeb canllawiau clir (yn y GDPR, yn ôl dehongliad gweithgor neu yn ôl awdurdod goruchwylio y DU), ystyrir eu bod yn y sector preifat at ddibenion y GDPR.

**6. Cyfrifoldebau o dan Y Rheoliad Cyffredinol ar Ddiogelu Data**

**6.1 Cyfrifoldebau Cyffredinol**

CTGC yw’r rheolydd data ac, mewn rhai amgylchiadau, y prosesydd data o dan y GDPR.

Y Bwrdd sydd â’r cyfrifoldeb cyffredinol o sicrhau arferion trin gwybodaeth da ac am adolygu a chymeradwyo’r polisi hwn.

Mae cyfarwyddwyr, rheolwyr a goruchwylwyr yn gyfrifol am ddatblygu ac annog arferion trin gwybodaeth da. Mae cyfrifoldebau wedi’u nodi mewn proffiliau swyddi.

Mae pob cyflogai sy’n rheoli neu’n prosesu data personol yn gyfrifol am sicrhau cydymffurfiaeth â deddfwriaeth diogelu data.

Mae cyflogeion yn gyfrifol am sicrhau bod eu data personol eu hunain yn gywir a chyfredol.

Bydd angen i gwsmeriaid sy’n darparu data personol gael gweld yr Hysbysiad Prosesu Teg ar adeg briodol.

**6.2 Swyddog Diogelu Data**

Mae’r SDD yn atebol i’r Uwch Dîm Rheoli am reoli data personol a sicrhau arfer da ac y gellir arddangos cydymffurfiaeth â deddfwriaeth. Mae hyn yn cynnwys:

* datblygu a gweithredu’r polisi hwn
* diogelwch a rheoli risg mewn cysylltiad â chydymffurfiaeth â’r polisi hwn
* meddu ar arbenigedd diogelu data
* cynnal adolygiad blynyddol o wybodaeth bersonol a ddelir i sicrhau bod rheswm busnes cadarn dros gadw’r wybodaeth honno.

Mae gan gyfarwyddwyr ac uwch reolwyr gyfrifoldeb ac atebolrwydd cyfwerth am reoli data personol yn y meysydd y maent hwy’n gyfrifol amdanynt.

Mae gan y SDD gyfrifoldebau penodol ar gyfer gweithdrefnau dylunio, er enghraifft am Geisiadau Mynediad Pwnc. Aelodau eraill o staff fydd yn gyfrifol am drin y rhain ond bydd y SDD yn darparu eglurhad i staff ar unrhyw agwedd ar ddeddfwriaeth a chydymffurfiaeth diogelu data.

**6.3 Cymhwysedd Polisi**

Disgwylir i bartneriaid ac unrhyw drydydd parti sy’n gweithio gyda CTGC, sydd â mynediad at wybodaeth bersonol, ddarllen, deall a chydymffurfio â’r polisi hwn. Ni all unrhyw drydydd parti gael mynediad at ddata personol a ddelir gan CTGC heb fod wedi ymrwymo i’n Cytundeb Cyflenwr yn gyntaf. (Mae hyn yn gosod rhwymedigaethau diogelwch a chyfrinachedd data sy’n llai llym na’r rhai y mae CTGC wedi ymrwymo iddynt, a rhydd yr hawl i CTGC archwilio cydymffurfiaeth â’r cytundeb).

Mae’r polisi hwn yn berthnasol i bob cyflogai ac eir i’r afael ag unrhyw achos o dorri rheoliadau’r GDPR neu’r polisi hwn yn unol â’r polisi Disgyblaeth. Os bydd trosedd; gellir hysbysu’r awdurdodau priodol.

**6.4 Atebolrwydd**

Mae’r GDPR yn cyflwyno’r egwyddor atebolrwydd sy’n datgan fod y Rheolydd Data yn gyfrifol am sicrhau cydymffurfiaeth yn ogystal ag arddangos bod pob gweithrediad prosesu yn cydymffurfio â’r GDPR. Yn benodol, mae’n ofynnol i Reolwyr Data:

* cynnal dogfennaeth angenrheidiol am yr holl weithrediadau prosesu;
* gweithredu mesurau diogelwch priodol;
* cyflawni Asesiadau o’r Effaith ar Brosesu Data (DPIA);
* cydymffurfio â’r gofynion ar gyfer hysbysiadau blaenorol, neu gymeradwyaeth gan awdurdodau goruchwyliol;
* penodi SDD pe byddai angen.

**7. Hysbysu**

Mae CTGC wedi hysbysu’r awdurdod goruchwyliol mai hwy yw’r Rheolydd Data a’u bod yn prosesu gwybodaeth benodol am wrthrychau data. Mae CTGC wedi nodi’r holl ddata personol y mae’n ei brosesu ac mae hyn wedi’i gynnwys yn y cofnod Data Personol a Dibenion.

Cedwir copi o’r hysbysiad awdurdod goruchwyliol (y cofnod ar y gofrestr) a chaiff ei adnewyddu’n flynyddol gan y SDD. Hysbysir unrhyw newidiadau i weithgareddau CTGC (e.e. o’r DPIA) gan y SDD.

Un dehongliad o’r GDPR yw na fyddwn mwyach yn gorfod cofrestru gydag awdurdod goruchwyliol y DU. Mae dehongliad arall yn dynodi y gallwn ddarparu llai o fanylion, er y bydd angen gwella cofnodion mewnol o weithgareddau prosesu. Bydd angen eglurhad llawn wrth wneud hysbysiad cyn y gwneir unrhyw newid i fanylion cofrestru CTGC.

**8. Datgelu data**

**8.1 Esemptiadau**

Mae’r GDPR yn caniatáu mathau penodol o ddatgeliadau nad oes angen cydsyniad ar eu cyfer, cyhyd ag y bydd angen y wybodaeth y gwnaed cais amdani am un neu fwy o’r dibenion canlynol:

* i ddiogelu diogelwch cenedlaethol;
* atal neu ganfod trosedd gan gynnwys dal ac erlyn troseddwyr;
* asesu neu gasglu treth;
* cyflawni swyddogaethau rheoleiddiol (gan gynnwys iechyd, diogelwch a llesiant personau yn y gwaith);
* atal niwed difrifol i drydydd parti;
* diogelu buddiannau hollbwysig yr unigolyn, e.e. sefyllfaoedd meddygol argyfyngus.

Mae’n rhaid i bob cais i ddarparu data am un o’r rhesymau hyn gael ei ategu gan y gwaith papur ‘cyfiawnhad’ priodol ac felly mae’n rhaid i bob datgeliad o’r fath gael ei awdurdodi’n benodol gan y SDD.

Mae’r esemptiad hwn yn caniatáu i ryddhau am y dibenion a nodwyd ac nid yw’n cwmpasu datgelu pob gwybodaeth bersonol ym mhob amgylchiad. Gofynnir y mathau canlynol o gwestiynau dilysu a chyfyngu:

* Ai'r person sy’n gofyn am y wybodaeth ydynt mewn gwirionedd?
* Ai eu bwriad yw atal neu ganfod trosedd, dal neu erlyn troseddwr neu asesu neu gasglu treth?
* Os na chaiff y wybodaeth ei rhyddhau, a fydd yn creu niwed arwyddocaol i atal trosedd neu ddal rhywun sy’n cael ei amau? (Mae’n rhaid bod risg y gallai’r ymchwiliad gael ei rhwystro.)
* Beth yw’r swm lleiaf o wybodaeth i’w galluogi i wneud eu gwaith?
* Beth arall sydd angen ei wybod er mwyn bod yn siŵr bod yr eithriad yn berthnasol?

**8.2 Rhannu Gwybodaeth**

Mae’n rhaid i CTGC sicrhau nad yw data personol yn cael ei ddatgelu i drydydd parti anawdurdodedig. Mae hyn yn cynnwys aelodau teulu, ffrindiau, cyrff y llywodraeth ac mewn amgylchiadau penodol, yr Heddlu. Dylai pob cyflogai arfer gofal pan ofynnir iddynt ddatgelu data personol a ddelir ar unigolyn i drydydd parti. Mae’n bwysig cofio a yw datgelu’r wybodaeth yn berthnasol, ac yn angenrheidiol, er mwyn cyflawni busnes CTGC.

Cytundebau Rhannu Gwybodaeth ar waith, e.e. gyda’r heddlu, cynghorau ac asiantaethau eraill, gan ddefnyddio protocolau cyffredin.

Nid oes gan aelodau’r Bwrdd unrhyw hawl i weld y data personol a gedwir ar ffeiliau, ac eithrio gyda chaniatâd ysgrifenedig yr unigolyn, nac unrhyw wybodaeth na fyddai’n cael ei datgelu i’r unigolyn, ac eithrio pan fydd angen gwneud hyn fel rhan o’u dyletswyddau.

Mae yna sefyllfaoedd pan fydd gwybodaeth yn cael ei hatal, er enghraifft pan fyddai’n datgelu rhywun arall nad ydynt wedi cydsynio i’r datgeliad, oni ellir ei olygu allan. Gofynnir i gyd-denantiaid gytuno i’w data gael ei rannu os bydd ond un ohonynt yn gwneud y cais, fel arall bydd yn rhaid golygu pob cyfeiriad at y cyd-denant arall o’r cais. Mae’n bosibl bod eithriadau eraill sy’n berthnasol yn benodol i wybodaeth iechyd.

Os bydd unrhyw bryderon y byddai achos o dorri’r GDPR, gwneir cais am orchymyn llys i’w gwneud yn ofynnol i ddatgelu a bydd y SDD yn cynghori ar hyn.

**8.3 Diogelu gwybodaeth**

Mae CTGC yn gweithio i ddiogelu plant, pobl ifanc ac oedolion sy’n agored i niwed rhag niwed. Mae gan CTGC ddyletswydd i hysbysu’r Gwasanaethau Cymdeithasol pan fydd risg i ddiogelwch unigolyn a rhannu gwybodaeth gyda hwy, p’un a yw’r pryderon wedi’u nodi gan neu wedi’u hadrodd yn uniongyrchol i staff. Y mathau o wybodaeth y gellir ei rhannu yw enwau, manylion cyswllt, gwybodaeth am iechyd corfforol neu feddyliol unigolyn a chysylltiadau ag eraill.

Mae gan CTGC weithdrefnau manwl sy’n cynnwys adrodd y wybodaeth hon sy’n dilyn protocolau rhannu gwybodaeth diogelu lleol gwahanol. Mae CTGC yn disgwyl i staff rhoi gwybod ar unwaith i’r arweinydd diogelu am unrhyw bryderon, a byddant hwy’n adrodd y wybodaeth yn unol â’r polisi Diogelu.

Mewn rhai amgylchiadau cyfyngedig penodol, mae’r Ddeddf yn caniatáu i ddata personol, hyd yn oed data sensitif, gael ei rannu heb i’r unigolyn fod yn ymwybodol o hyn.

**9. Marchnata uniongyrchol**

Gall CTGC ddefnyddio data personol ar gyfer marchnata uniongyrchol (gan gynnwys i bartneriaethau busnes) mewn cysylltiad â’i weithgareddau. Mae hyn yn cynnwys e-bost a thestun, galwadau ffôn ac ymgyrchoedd postio uniongyrchol. Sicrheir cydsyniad ar yr adeg y bydd yr unigolyn yn darparu’r data personol. Gall unrhyw unigolyn arfer eu hawl, ar unrhyw adeg, optio allan i’w data personol gael ei ddefnyddio yn y dull hwn a bydd CTGC yn cydsynio â hyn.

Mae ein systemau cyfrifiadurol yn cofnodi dewisiadau cysylltu preswylwyr (os a sut) ac wrth gwrs, dilynir y ceisiadau hyn.

**10. Cyflogeion**

Cesglir data personol sy’n gysylltiedig â chyflogeion o geisiadau swyddi a phryd bynnag y bydd data yn cael ei ddiweddaru drwy’r adran Adnoddau Dynol neu’r Gyflogres. Mae’r ffurflen cais am swydd yn datgan y bydd y wybodaeth sy’n cael ei chasglu yn gwbl gyfrinachol ac y bydd ond yn cael ei defnyddio at ddibenion personél a gweinyddu cyflog, neu fel arall mewn cysylltiad â busnes CTGC. Mae hyn yn cynnwys defnyddio data at ddibenion monitro, a gwirio’r defnydd o e-bost a’r rhyngrwyd a gwirio teledu cylch cyfyng ar gyfer ymchwiliadau troseddol, dibenion disgyblu ac iechyd a diogelwch mewn achos o ddigwyddiad. Mae hyn hefyd yn ymddangos mewn contractau cyflogaeth. Ni chedwir data am fwy na sydd angen, yn unol â Pholisi Cadw Data CTGC.

Bydd CTGC yn cydymffurfio â’r ceisiadau canlynol am ddata personol:

* Gan asiantau sydd wedi’u hawdurdodi gan y cyflogai e.e. ceisiadau morgais, geirdaon. Dylai’r cyflogai gadarnhau yn ysgrifenedig y bydd y wybodaeth yn cael ei datgelu.
* At ddibenion gorfodi’r gyfraith (h.y. gan yr heddlu er mwyn atal neu ganfod trosedd, asesu neu gasglu unrhyw dreth gan Cyllid a Thollau EM, neu’r Asiantaeth Cynnal Plant neu Gynhaliaeth Plant). Caniateir datgeliad pan fyddai methiant i wneud y datgeliad yn debygol o niweidio un o’r dibenion hyn. Ym mhob achos, cyflwynir diben y cais yn ysgrifenedig.
* Ar gyfer unrhyw broses gyfreithiol orfodol arall.
* Os bydd angen ar frys, ar gyfer atal anaf a niwed i iechyd.
* Gan swyddogion undebau llafur. Gofynnir i’r cyflogai gadarnhau yn ysgrifenedig.
* Gan ffynonellau allanol a nodwyd yn benodol, e.e. gweinyddwyr pensiwn, er mwyn gweinyddu cynlluniau buddiannau mewnol.

Mae gan gyflogeion yr hawl i weld eu data personol, ond mae’n rhaid iddynt roi rhybudd rhesymol i ddarparu mynediad. Mae gan gyflogeion hawl hefyd i wybod at ba ddibenion y bydd eu data personol yn debygol o gael eu defnyddio a’r derbynwyr tebygol (neu ddosbarth o dderbynwyr). Mae’r wybodaeth ganlynol wedi’i heithrio rhag cael ei datgelu:

* Gellir diogelu geirdaon oherwydd byddai’n datgelu gwybodaeth sy’n gysylltiedig â thrydydd parti y gellir eu hadnabod.
* Data personol i’w ddefnyddio ar gyfer gwaith rhagweld neu gynllunio rheolwyr, pe byddai ei ddatgelu yn debygol o niweidio’r broses o gyflawni’r busnes neu weithgarwch yn unig.
* Cofnodion sy’n gysylltiedig ag unrhyw drafodaethau gyda’r cyflogai, pe byddai datgeliad yn debygol o niweidio’r trafodaethau penodol hynny.
* Os yw’n ymwneud â datgelu gwybodaeth sy’n gysylltiedig â thrydydd parti y gellir eu hadnabod, oni fydd y trydydd parti wedi cydsynio neu ei bod yn rhesymol cydymffurfio heb eu cydsyniad hwy. Os na fydd yr opsiynau hyn yn bosibl, bydd y data yn cael ei olygu, i ddiogelu hunaniaeth trydydd parti. Gwneir datgeliad os gofynnir am gofnod iechyd a bod y trydydd parti yn weithiwr iechyd proffesiynol sydd wedi cydymffurfio neu gyfrannu ato.

Ni all cyflogai atal prosesu sydd ei angen ar gyfer cyflawni contract y mae’r cyflogai yn rhan ohono.

Bydd gwybodaeth bersonol am gyflogai a roddir i aelodau’r bwrdd yn cael ei golygu i ddileu unrhyw wybodaeth am drydydd parti.

**11. Cyflenwyr a Chontractwyr**

Mae CTGC yn cyflogi contractwyr amrywiol i gyflawni tasgau a gwasanaethau ar ei ran; mae gan rai ohonynt angen gwirioneddol i ddefnyddio data personol ein preswylwyr. Gelwir contractwyr o’r fath yn broseswyr data.

Os yw contractwr yn debygol o fod yn brosesydd data, mae’n rhaid cynnwys cyfres safonol o is-gymalau yn y ddogfen dendr. Mae’r rhain yn nodi’r gofynion sylfaenol sydd eu hangen ar statws diogelu data'r contractwr. Rhoddir manylion llawn yn y polisi Diogelu Data - Is-gymal a Chytundeb Tendrau Cyflenwyr.

Mae’n rhaid i’r contractwr sy’n llwyddo i ennill y contract ymrwymo mewn Cytundeb Prosesu Diogelu Data sy’n nodi’r safonau a’r rhwymedigaethau y mae CTGC yn eu disgwyl wrth brosesu data personol. Mae’r cytundeb hirach hwn hefyd yn y polisi Diogelu Data – Is-gymal a Chytundeb Tendrau Cyflenwyr.

Mae’n ofynnol i gontractwyr presennol lofnodi atodiad i’r contract i ddweud y byddant yn cydymffurfio â pholisïau GDPR a CTGC am eu bod yn berthnasol i’r contract.

**12. Asesiad o’r Effaith ar Risg a Diogelu Data**

Mae’n bosibl y bydd risgiau sy’n gysylltiedig â phrosesu mathau penodol o ddata personol, y mae’n rhaid i CTGC eu hasesu drwy Asesiad o’r Effaith ar Ddiogelu Data (DPIA). Gall DPIA gwmpasu prosesu data personol yn fewnol a’r prosesu a wneir gan sefydliadau eraill ar ran CTGC, Gweler y weithdrefn Asesiad o Effaith ar Breifatrwydd.

Dylai systemau a thechnolegau newydd fod yn destun archwiliad eu bod wedi’u dylunio i gyflawni gofynion GDPR; ac os nad ydynt efallai y bydd angen rheolaethau ychwanegol. Os yw cwmpas, natur, cyd-destun a dibenion y prosesu yn debygol o arwain at risg uchel i hawliau a rhyddid, bydd CTGC, cyn y prosesu, yn cynnal DPIA o effaith y gwaith prosesu arfaethedig. Gallai DPIA unigol fynd i’r afael â chyfres o weithrediadau prosesu tebyg sy’n cyflwyno risgiau uchel tebyg.

Pan fydd yn amlwg, o ganlyniad i DPIA, bod CTGC ar fin dechrau prosesu data personol a allai niweidio a/neu beri gofid i wrthrychau’r data, mae’n rhaid i’r SDD adolygu’r penderfyniad a ddylai CTGC barhau i brosesu ai peidio. Bydd y SDD, os bydd pryderon arwyddocaol, yn uwchgyfeirio’r mater i’r awdurdod goruchwyliol.

Gellir dewis rheolaethau priodol o, er enghraifft, ISO27001 (cyfres o safonau diogelwch gwybodaeth) a ffynonellau arfer da i leihau’r risg i lefel dderbyniol a sicrhau cydymffurfiaeth â GDPR.

Er mwyn diogelu cyflogeion a chontractwyr rhag risg wrth weithio yng nghartrefi preswylwyr, mae gan CTGC system i adnabod pobl a allai fygwth diogelwch cyflogeion ac eraill. Mae’r wybodaeth hon yn gyfrinachol ac ni chaiff ei datgelu y tu allan i CTGC oni fydd ei hangen i sicrhau iechyd a diogelwch contractwyr a chyflenwyr eraill. Bydd yn destun adolygiad a bydd yn cael ei chadw’n gyfredol a chywir.

**13. Torri diogelwch**

Mae’n rhaid i unrhyw gyflogai sy’n amau achos o dorri diogelwch data, hysbysu’r SDD ar unwaith, a fydd yn ymchwilio yn dilyn trafodaeth gydag Ysgrifennydd y Cwmni, a fydd yn dirprwyo yn absenoldeb y SDD. Bydd achosion difrifol o dorri diogelwch yn cael eu hadrodd i’r awdurdod goruchwyliol gan ddefnyddio’r weithdrefn Hysbysiad Torri.

Mae achos o dorri diogelwch yn cynnwys (ond nid yw wedi’i gyfyngu i):

* Datgelu data personol neu ddata personol sensitif i berson anawdurdodedig.

• Camddefnyddio cyfrineiriau neu roi mynediad i gyfrineiriau.

• Camddefnyddio data personol neu sensitif neu wybodaeth busnes sensitif, hyd yn oed os cafwyd mynediad cyfreithiol iddi.

• Caniatáu, sicrhau neu geisio sicrhau mynediad anawdurdodedig i systemau.

* Gweithredu y tu allan i God Ymddygiad Cyflogeion a pholisïau, gweithdrefnau, cyngor a chanllawiau CTGC ar ddiogelu data neu ddiogelu gwybodaeth.

• Colli, difrodi neu ddinistrio data personol yn ddamweiniol.

**14. Cofnodion a Chynnal a Chadw**

**14.1 ‘Cofrestr Asedau Gwybodaeth’**

Mae CTGC wedi sefydlu Cofrestr Asedau Gwybodaeth i gofnodi gweithgareddau prosesu data personol, sy’n diffinio:

* diben y prosesu;
* y camau amrywiol sy’n gysylltiedig â’r prosesu;
* pa ddata sy’n cael ei brosesu;
* i bwy mae’r data yn gysylltiedig;
* mesurau technegol a sefydliadol a gymerwyd i ddiogelu’r data;
* sut y rhoddir cydsyniad/defnyddir y porth prosesu;

Rhoddir manylion llawn yn y weithdrefn Cofrestr Asedau Gwybodaeth ar wahân.

**14.2 Cadw a gwaredu data**

Ni fydd CTGC yn cadw data personol ar ffurf sy’n galluogi i wrthrychau’r data gael eu datgelu am gyfnod hwy na’r hyn y bydd CTGC yn ystyried sy’n angenrheidiol (mewn cysylltiad â’r diben(ion) y casglwyd y data yn wreiddiol ar ei gyfer/eu cyfer).

Gall CTGC storio data am gyfnodau hwy os bydd y data yn cael ei brosesu at ddibenion archifo yn unig er budd y cyhoedd, dibenion gwyddonol neu ymchwil hanesyddol neu ddibenion ystadegol, yn ddarostyngedig i weithredu mesurau technegol a sefydliadol priodol er mwyn diogelu hawliau a rhyddid gwrthrych y data.

Bydd y cyfnod cadw ar gyfer pob categori o ddata personol yn cael ei nodi yn y polisi Cadw Dogfennau a Data, yn ogystal â’r meini prawf a ddefnyddiwyd i bennu’r cynnwys hwn, gan gynnwys unrhyw rwymedigaethau statudol i gadw’r data.

Mae’n rhaid gwaredu data personol mewn ffordd sy’n diogelu “hawliau a rhyddid” gwrthrychau’r data (e.e. llarpio, gwaredu fel gwastraff cyfrinachol, dileu electronig diogel) ac yn unol â’r polisi Cadw Dogfennau a Data.

**15. Hyfforddiant**

Bydd yn ofynnol i bob aelod o staff ac aelodau’r bwrdd ddarllen a deall y polisi hwn fel rhan o’u hyfforddiant sefydlu. Bydd staff yn derbyn hyfforddiant yn rheolaidd ar y polisi hwn, gan gynnwys ar eu hawliau eu hunain. Rhoddir hyfforddiant mwy manwl ar drin ceisiadau mynediad pwnc yn unol â’r Ddeddf i aelodau o staff perthnasol. Bydd y SDD yn derbyn hyfforddiant mwy arbenigol.

**16. Monitro ac adrodd**

Mae’r SDD yn monitro cydymffurfiaeth â’r polisi hwn ac yn hysbysu ysgrifennydd y Cwmni ynghylch unrhyw achos o dorri polisi. Mae CTGC yn ystyried bod unrhyw wybodaeth bersonol a ddarperir i’w cwsmeriaid, staff neu gontractwyr yn gyfrinachol a bydd unrhyw ddatgeliad anawdurdodedig yn cael ei drin yn ddifrifol iawn.

Ystyrir bod achos bwriadol o dorri’r polisi hwn yn drosedd ddisgyblu ddifrifol a gallai arwain at gymryd camau disgyblu a allai arwain at ddiswyddo. Gallai staff wynebu atebolrwydd troseddol mewn rhai amgylchiadau. Mae’n ofynnol i staff hysbysu’r SDD pan amheuir achos o dorri’r polisi.

|  |  |
| --- | --- |
| **Polisïau cysylltiedig**  **Polisi** | **Dyddiad** |
|  |  |
| Polisi Cadw Data  *Polisïau GDPR*  Polisi Preifatrwydd DD (a Hysbysiad Prosesu Teg)  Polisi Cyfrifoldebau DD Cyflenwyr |  |

**Atodiad A**

**Rhestr o Ddiffiniadau**

**Atodiad A – Diffiniadau**

**1 Awdurdod Goruchwyliol** – yr awdurdod cyhoeddus annibynnol a sefydlwyd gan aelod-wladwriaeth i weinyddu a rheoleiddio’r GDPR. Yr awdurdod presennol yn y DU yw Swyddfa’r Comisiynydd Gwybodaeth, a all barhau gyda’r un enw a rôl ar gyfer y GDPR.

**2 Cwmpas perthnasol –** mae’r GDPR yn prosesu data personol yn gyfan gwbl, neu’n rhannol, drwy ddulliau awtomataidd (h.y. drwy gyfrifiadur) ac i brosesu data personol drwy ddulliau eraill nad ydynt yn awtomataidd (h.y. cofnodion papur) sy’n ffurfio rhan o system ffeilio ‘strwythuredig’ neu y bwriedir iddynt ffurfio rhan o system ffeilio.

**3 Cwmpas tiriogaethol –** bydd y GDPR yn berthnasol i bob rheolydd sydd wedi’i sefydlu yn yr UE (Undeb Ewropeaidd) sy’n prosesu data personol gwrthrychau data. Bydd hefyd yn berthnasol i reolwyr y tu allan i’r UE sy’n prosesu data personol er mwyn cynnig nwyddau a gwasanaethau, neu i fonitro ymddygiad gwrthrychau data sy’n preswylio yn yr UE.

**4** **Cydsyniad gwrthrych y data** – mae hyn yn golygu unrhyw arwydd a roddir yn rhydd, penodol, gwybodus a diamwys o ddymuniadau gwrthrych y data y mae ef neu hi, drwy ddatganiad neu drwy weithred gadarnhaol glir, yn cynrychioli cytundeb i brosesu data personol.

**5** **Data personol** – unrhyw wybodaeth sy’n gysylltiedig â pherson naturiol y gellir eu hadnabod neu sy’n adnabyddadwy (‘gwrthrych data’); person naturiol adnabyddadwy yw person y gellir eu hadnabod, yn uniongyrchol neu’n anuniongyrchol, yn arbennig drwy gyfeiriad at adnabyddwr, er enghraifft enw, rhif adnabod, data lleoliad, adnabyddwr ar-lein neu un neu fwy o ffactorau sy’n benodol i hunaniaeth gorfforol, seicolegol, genetig, meddyliol, economaidd, diwylliannol neu gymdeithasol y person naturiol hwnnw. Mae’n cwmpasu gwybodaeth am bobl fyw, sy’n cael ei storio ar gyfrifiadur neu mewn system ffeilio bapur drefnus, system teledu cylch cyfyng, camera digidol neu recordiadau sain a delweddau digidol.

**6** **Data sensitif/Categorïau arbennig o ddata personol** – data personol sy’n datgelu tarddiad hiliol neu ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, neu aelodaeth ag undeb llafur, a phrosesu data genetig, data biometreg at y diben o adnabod person naturiol yn unigryw, data sy’n ymwneud ag iechyd neu ddata sy’n ymwneud â bywyd rhywiol neu gyfeiriadedd rhywiol person naturiol.

**7 Gwrthrych data** – unrhyw unigolyn byw sy’n destun data personol a ddelir gan sefydliad.

**8** **Plentyn –** mae’r GDPR yn diffinio plentyn fel unrhyw un o dan 13 oed. Bydd prosesu data personol plentyn ond yn gyfreithlon os bydd cydsyniad rhieni neu ofalwr wedi’i sicrhau. Bydd y rheolydd yn gwneud ymdrechion rhesymol i ddilysu mewn achosion o’r fath bod cydsyniad wedi’i roi neu ei awdurdodi gan y sawl â chyfrifoldeb rhieni dros y plentyn.

**9 Proffilio** – mae hyn yn unrhyw fath o brosesu data personol awtomataidd, y bwriedir iddo werthuso rhai agweddau personol penodol sy’n gysylltiedig â pherson naturiol, neu i ddadansoddi neu ragweld perfformiad y person hwnnw yn y gwaith, eu sefyllfa economaidd, lleoliad, iechyd, dewisiadau personol, dibynadwyedd neu ymddygiad. Mae cysylltiad rhwng y diffiniad hwn â hawl gwrthrych y data i wrthwynebu i unrhyw broffilio a hawl i gael ei hysbysu ynglŷn â phresenoldeb proffilio, mesurau sy’n seiliedig ar broffilio ac effeithiau arfaethedig proffilio ar yr unigolyn.

**10 Prosesu –** mae hyn yn unrhyw ffurf o brosesu data personol yn awtomataidd, y bwriedir iddo werthuso rhai agweddau personol penodol sy’n gysylltiedig â pherson naturiol, neu i ddadansoddi neu ragweld perfformiad y person hwnnw yn y gwaith, eu sefyllfa economaidd, lleoliad, iechyd, dewisiadau personol, dibynadwyedd neu ymddygiad. Mae cysylltiad rhwng y diffiniad hwn â hawl gwrthrych y data i wrthwynebu i unrhyw broffilio a hawl i gael ei hysbysu ynglŷn â phresenoldeb proffilio, mesurau sy’n seiliedig ar broffilio ac effeithiau arfaethedig proffilio ar yr unigolyn.

**11 Rheolydd Data** – person naturiol neu gyfreithiol, awdurdod cyhoeddus, asiantaeth neu gorff arall sy’n penderfynu dibenion ac ystyr prosesu data personol.

**12 Sefydliad –** prif sefydliad y rheolydd yn yr UE fydd y lle y bydd y rheolydd yn gwneud y prif benderfyniadau ynglŷn â diben a dulliau ei weithgareddau prosesu data. Prif sefydliad prosesydd yn yr UE fydd ei ganolfan weinyddol. Os bydd rheolydd wedi’i leoli y tu allan i’r UE, bydd yn rhaid iddynt benodi cynrychiolydd yn yr awdurdodaeth y bydd y rheolydd yn gweithredu ar ran y rheolydd ac yn delio ag awdurdodau goruchwyliol.

**13 System ffeilio** – unrhyw gyfres strwythuredig o ddata personol sy’n hygyrch yn ôl meini prawf penodol, p’un a yw’n ganolog, wedi’i ddatganoli neu wedi’i ddosbarthu ar sail swyddogaethol neu ddaearyddol. Mae “strwythuredig” yn cwmpasu unrhyw system gyfrifiadurol neu system â llaw sydd â system ‘fynegeio gyflym’.

**14 Torri data personol** – torri diogelwch sy’n arwain at achos damweiniol, neu anghyfreithlon o ddinistrio, colli, addasu, datgelu anawdurdodedig, neu fynediad at, ddata personol sydd wedi’i drosglwyddo, storio neu ei brosesu fel arall. Mae rhwymedigaeth ar y rheolydd i adrodd achos o dorri data personol i’r awdurdod goruchwyliol, pan fydd yr achos o dorri yn debygol o gael effaith andwyol ar ddata personol neu breifatrwydd gwrthrych y data.

**15 Trydydd parti** – person naturiol neu gyfreithlon, awdurdod, asiant neu gorff cyhoeddus ar wahân i wrthrych, rheolydd, prosesydd y data, a phersonau sydd, o dan awdurdod uniongyrchol y rheolydd neu’r prosesydd, wedi’u hawdurdodi i brosesu data personol.