Canllawiau Diogelu Data a Diogelwch Data i Gynhyrchwyr

1. Cyflwyniad

Mae'r canllawiau hyn yn gosod y rhagofalon yr argymhellir y dylai pob cwmni cynhyrchu eu gweithredu er mwyn diogelu data personol gan gynnwys data categori arbennig (y cyfeirid atynt gynt fel 'data personol sensitif'), yng ngoleuni'r Rheoliad Cyffredinol ar Ddiogelu Data (GDPR), a ddaeth i rym ar 25 Mai 2018. Gweithredir hyn yn y Deyrnas Unedig o dan DDD 2018 (DDD 2018).

Mae'r Canllawiau hyn yn ddogfen fyw, ac fe gyhoeddir diweddariadau iddi o bryd i'w gilydd.

Y GDPR yw'r ddeddfwriaeth Ewropeaidd newydd ar ddiogelu data ac mae DDD 2018 yn disodli DDD 1998. Trwy weithredu'r GDPR, bwriedir rhoi gwell rheolaeth i unigolion dros eu data personol eu hunain. Mae'r GDPR yn sefydlu rhai egwyddorion a chysyniadau newydd, gan gynnwys hawliau newydd i unigolion.

Diben y canllawiau hyn yw darparu cyngor ymarferol i gynorthwyo cynhyrchwyr i ddiogelu data personol a thrwy hynny ddiogelu cwmnïau cynhyrchu rhag sancsiynau sifil a/neu droseddol, a rhag difrod i'w henw da oherwydd colli neu ddifrodi data personol neu ddata categori arbennig, neu oherwydd datgelu data o'r fath heb awdurdod.

Mae'n bwysig bod pob uwch-aelod staff pob cwmni cynhyrchu yn darllen y canllawiau hyn, a'u bod yn darparu cymorth ac arweiniad ymarferol i holl staff y cwmni. Argymhellir bod un uwch-berson, sef Rheolwr Data neu Swyddog Diogelu Data, yn ymgymryd â'r cyfrifoldeb cyffredinol am bolisi ac ymarfer diogelu data ledled y cwmni. Dylai manylion cyswllt yr uwch-berson hwnnw fod ar gael yn hwylus i'r holl staff ac i unrhyw unigolyn sydd ag ymholiad ynghylch y modd y mae'r cwmni yn trin ei ddata personol.

Mae gwefan Swyddfa'r Comisiynydd Gwybodaeth, sef y corff sy'n rheoleiddio diogelu data yn y Deyrnas Unedig, yn darparu gwybodaeth ddefnyddiol am y rhan fwyaf o faterion cydymffurfiaeth. Os bydd gennych ymholiadau manwl ynghylch materion penodol, mae'n debygol y gall llinell gymorth teleffon Swyddfa'r Comisiynydd Gwybodaeth ddarparu atebion. Hwyrach hefyd y dylech ystyried a ddylai aelodau o'r staff, neu'ch contractwyr, gwblhau sesiwn neu gwrs o hyfforddiant, i'w helpu i ddeall eich rhwymedigaethau o dan y GDPR.

Sylwer hefyd ar y Canllawiau Diogelu Data a Diogelwch Data i Griw Cynhyrchu a atodir, sy'n darparu cyngor a chymorth ymarferol ar gyfer eich criwiau cynhyrchu**,** a fydd yn trin data personol a data categori arbennig pobl sy'n fyw.

2. Pwy sy'n gyfrifol am y GDPR yn y DU?

Swyddfa'r Comisiynydd Gwybodaeth sy'n gyfrifol am orfodi'r GDPR yn y DU. Mae gan Swyddfa'r Comisiynydd Gwybodaeth bwerau i gynnal ymchwiliadau troseddol, i gymryd camau gorfodi ac i osod dirwyon.

3. A oes angen i mi gofrestru gyda Swyddfa'r Comisiynydd Gwybodaeth mewn perthynas â'r GDPR?

Os ydych yn casglu a phrosesu data personol, mae'n dra thebygol y bydd angen i'ch cwmni dalu ffi ar gyfer cofrestru gyda'r Comisiynydd Gwybodaeth, er mwyn bod ar gofrestr y Comisiynydd. Mae hyn yn ofyniad cyfreithiol, a gallai peidio â thalu ffi cofrestru achosi dirwy.

Os oedd angen i chi gofrestru o dan y DDD 1998, mae'n debygol y bydd angen i chi gofrestru a thalu'r ffi berthnasol o dan y strwythur ffioedd newydd ar gyfer rheolwyr data, a gynhwysir yn **Rheoliadau Diogelu Data (Ffioedd a Gwybodaeth) 2018**. Daeth y Rheoliadau hyn i rym ar 25 Mai 2018, i gyd-ddigwydd â gweithredu'r GDPR a'r DDD 2018.

(Nid yw hyn yn golygu bod rhaid i chi ail-gofrestru a thalu'r ffi newydd ar 25 Mai. Nid oes rhaid i Reolwyr Data sydd â chofrestriad (neu hysbysiad) cyfredol eisoes o dan y DDD ail-gofrestru na thalu'r ffi newydd hyd nes daw eu cofrestriad cyfredol i ben).

Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar ffioedd am gofrestru yn: https://ico.org.uk/for-organisations/register/

4. Pa bethau sy'n berthnasol i'r GDPR?

Mae'r GDPR yn berthnasol i ddata personol ac i weithgareddau prosesu a gyflawnir gan gwmnïau o fewn yr Undeb Ewropeaidd, yn ogystal â chwmnïau y tu allan i'r Undeb Ewropeaidd sy'n cynnig nwyddau neu wasanaethau i unigolion yn yr Undeb Ewropeaidd.

5. Beth yw data personol?

Mae dau fath o ddata, sef **data personol** a **data categorïau arbennig**. Mae data categori arbennig, er hynny, hefyd yn ddata personol, ond rhaid eu prosesu o dan amodau ychwanegol (gan ei bod yn debygol y bydd arnoch angen amod ychwanegol yn ogystal ar gyfer data nad ydynt yn ddata categori arbennig). Esbonnir hyn ymhellach ym mhwynt 5.2 isod.

5.1 Data personol

Data personol yw data sy'n ymwneud ag **unigolyn sy'n fyw**, ac y gellir eu cysylltu'n uniongyrchol neu'n anuniongyrchol â'r person hwnnw, neu ddata y gellir adnabod yr unigolyn hwnnw ar eu sail os darllenir y data personol ar y cyd â gwybodaeth arall sydd ar gael yn hwylus. Gall hyn gynnwys **unrhyw un neu ragor o'r manylion canlynol**: enw'r unigolyn, ei gyfeiriad, delweddau, rhifau teleffon, cyfeiriadau e-bost personol, dyddiad geni, manylion banc a chyflogres, ei berthynas agosaf *(next of kin)*, manylion pasbort ac ati. Mae'r diffiniad o ddata personol yn GDPR yn un eang, sy'n egluro y gall dynodydd adnabod ar-lein, megis cyfeiriad IP, fod yn ddata personol. Gellir pennu bod data dan ffugenw, hyd yn oed, yn ddata personol, yn dibynnu ar ba mor hawdd fyddai priodoli'r data hynny i unigolyn penodol.

5.2 Beth yw data categori arbennig?

Mae data categori arbennig (a elwid gynt yn 'Ddata Personol Sensitif' o dan y DDD 1998) yn ymwneud â tharddiad hiliol neu ethnig unigolyn, ei safbwyntiau gwleidyddol, credoau crefyddol, aelodaeth o undeb llafur, iechyd corfforol neu feddyliol a'i fywyd neu'i dueddiadau rhywiol. Mae'n cynnwys data genetig a biometrig yn ogystal. Dywed Erthygl 9 o'r GDPR fod prosesu data categori arbennig wedi ei wahardd oni ellir bodloni un neu ragor o'r seiliau cyfreithlon sydd yn yr Erthygl honno. **Nid yw** data personol am droseddau a chollfarnau troseddol bellach yn gynwysedig yn y diffiniad hwn, ond gweithredir rhagofalon tebyg ynglŷn â'u prosesu (rhoddir manylion yn adran 5.3 o'r canllawiau hyn).

5.3 Beth yw data troseddau?

Mae'r cysyniad o ddata troseddau yn cynnwys data am honiadau o droseddu; achosion llys a chollfarnau troseddol a throseddau; neu fesurau diogelwch perthnasol.

Pennir rhagofalon ar wahân yn Erthygl 10 o'r GDPR ar gyfer Data Troseddau, a hefyd o dan y DDD 2018. Er mwyn prosesu data personol am gollfarnau troseddol neu droseddau, rhaid i chi gael sail gyfreithlon o dan Erthygl 6, ynghyd â naill ai awdurdod cyfreithiol neu awdurdod swyddogol ar gyfer y prosesu, o dan Erthygl 10.

Ni chaiff cwmnïau cynhyrchu gasglu gwybodaeth am droseddau ac eithrio pan fo'n briodol gwneud hynny oherwydd natur y rôl dan sylw, er enghraifft, yn rhan o broses recriwtio at y diben o amddiffyn plant, pan fo hawl gyfreithiol gennych i wneud gwiriadau manylach/safonol neu ofyn am wiriadau sylfaenol *(enhanced, standard, basic DBS Check)* gan y Gwasanaeth Datgelu a Gwahardd (os mai at ddiben diogelu plant y cesglir yr wybodaeth, gellir dibynnu ar Atodlen 1, Rhan 2, paragraff 10 neu 18 o'r DDD 2018). Sylwch, os gwelwch yn dda, ar gyfer y naill neu'r llall o'r seiliau hyn, mae'n ofynnol bod dogfen bolisi briodol wedi ei mabwysiadu, yn unol ag Atodlen 1, Rhan 2, paragraff 5(1), ac Atodlen 1, Rhan 4 o'r DDD 2018.

Dylech wybod na chewch gadw cofrestr gynhwysfawr o gollfarnau troseddol oni fyddwch yn gwneud hynny yn rhinwedd rôl swyddogol.

Os ydych yn bwriadu ymdrin â'r math hwn o ddata ar gyfer eich rhaglen, darllenwch y fersiwn ddiweddaraf o ganllawiau Swyddfa'r Comisiynydd Gwybodaeth. Os byddwch yn ansicr, dylech ofyn am gyngor cyfreithiol a siarad gyda'r darlledwr sy'n eich comisiynu:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

6. Lle y deuir o hyd i ddata personol?

Bydd eich cyflogeion a'ch gweithwyr llawrydd yn cael mynediad i ddata personol, neu'n dod ar eu traws yn feunyddiol, o lawer o ffynonellau ac mewn gwahanol ffurfiau. Er enghraifft, byddant yn cael data personol gan gyflogeion, cyfranwyr, cyflenwyr a chontractwyr, yn awr fel yn y gorffennol a'r dyfodol.

Bydd data personol yn bresennol yn eich rhaglenni, deunydd crai *(rushes)*, neu mewn llythyrau, negeseuon e-bost, gohebiaeth, cofnodion galwadau, triniaethau a threfnau rhaglenni, curricula vitarum, darnau ffilm cylch cyfyng, cytundebau, ffurflenni rhyddhau a ffurflenni cais cyfranwyr, taflenni galwadau, P-as-Cs, gwiriadau'r gwasanaeth datgelu a gwahardd, cofnodion meddygol, anfonebau, archebion prynu, deunydd crai *(rushes)* â chapsiynau, cyfriflenni banc, rhestrau cyflogeion, ar wefannau ac mewn geirdaon cyflogeion. Gall y data personol fod **ar ffurf copïau caled**, sef dogfennau papur gwreiddiol neu gopïau ohonynt, ffotograffau neu ffilm; neu **ar ffurf electronig** mewn cyfrifiaduron personol, gliniaduron, ffonau symudol neu BlackBerry, neu gofion bach.

Wrth baratoi i gasglu data personol, dylid cymryd gofal i gyfyngu'r data personol a gesglir i'r hyn sy'n angenrheidiol mewn gwirionedd. Peidiwch â chasglu data personol yn unig rhag ofn y bydd arnoch eu hangen yn unig. Er enghraifft, mae'n annhebygol y byddai arnoch angen gwybodaeth am hanes rhywiol cyfrannwr, oni fyddai hynny'n berthnasol i'r rhaglen.

Gan fod y diffiniadau o ddata personol yn eang, wrth wneud rhaglen, gallech fod yn prosesu data categori arbennig yn ogystal â data personol arall.

Os byddwch yn trin data personol, bydd angen i chi sefydlu eich lefel o gyfrifoldeb, a bydd hynny'n seiliedig ar ba un ai rheolydd data ynteu brosesydd data ydych. Mae pa un ai rheolydd data ynteu brosesydd data ydych yn fater o ffaith, ac yn dibynnu ar ba un ai chi sy'n penderfynu modd a diben y prosesu data ai peidio. Ni chaniateir i sefydliad neu gwmni benderfynu ei statws ei hun yn hyn o beth er mwyn osgoi rhwymedigaethau penodol.

7. A ydych yn brosesydd data ynteu'n rheolydd data?

Rheolwyr data sydd â'r cyfrifoldeb eithaf am gydymffurfiaeth mewn perthynas â data personol, a rhaid iddynt allu dangos eu bod yn cydymffurfio â'r egwyddorion rheoli data (gweler adran 8). Dylech wybod y gall cwmni cynhyrchu fod yn rheolydd data ac yn brosesydd data mewn perthynas â data personol, neu'n gyd-reolydd data personol, ond ni all fod yn rheolydd data ac yn brosesydd data yr un pryd mewn perthynas â'r un data personol.

7.1. Beth yw rheolydd data?

Rheolydd data sy'n pennu'r dibenion o brosesu data personol a'r modd y'u prosesir. Mewn rhai amgylchiadau, maent yn "rheolwyr ar y cyd' neu'n 'gyd-reolwyr'. Os ydych yn rheolydd data ac yn cyfarwyddo prosesydd data i gyflawni gweithgareddau prosesu ar eich rhan, mae'r GDPR yn gosod rhwymedigaethau arnoch i sicrhau bod eich contractau gyda phroseswyr data yn cydymffurfio â'r GDPR. O dan y GDPR, ar y rheolydd data y mae'r cyfrifoldeb am gydymffurfio ac arddangos cydymffurfiaeth ag egwyddorion diogelu data y GDPR. Bydd cynhyrchwyr er enghraifft, yn rheolwyr data mewn perthynas â'r holl ddata personol a brosesir wrth ddatblygu a chynhyrchu'r rhaglenni y comisiynir hwy i'w cynhyrchu, oni phennir a chytunir yn wahanol rhwng y partïon, mewn ysgrifen.

7.2. Beth yw prosesydd data?

Prosesydd data sy'n gyfrifol am brosesu data personol ar ran rheolydd data. Os ydych yn brosesydd data, mae'r GDPR yn gosod rhwymedigaethau cyfreithiol penodol arnoch; er enghraifft, mae'n ofynnol eich bod yn cadw cofnodion o ddata personol a gweithgareddau prosesu ac adrodd yn brydlon a di-oed wrth y rheolydd data am unrhyw doriad

diogelwch data sy'n ymwneud â data personol. Mae'n ofynnol hefyd eich bod yn gweithredu mesurau technegol a threfniadol priodol ar gyfer diogelu a chadw data personol. Sylwch, os gwelwch yn dda, nad proseswyr data ar gyfer cwmni yw ei gyflogeion; pan fo cwmni yn rheolydd data, a chyflogai yn gweithredu ar ran y cwmni hwnnw, mae'r cyflogai yn gweithredu fel rheolydd data.

7.3 <u>Beth os wyf yn cyfarwyddo trydydd parti i drin data personol ar gyfer y Rhaglen?</u>

Os ydych yn defnyddio trydydd parti i gasglu, prosesu neu waredu data personol ar eich rhan, ac nad yw'r parti hwnnw yn pennu diben a modd y prosesu, bydd y parti hwnnw yn brosesydd data.

Enghraifft o brosesydd data o'r fath fyddai cwmni a ddefnyddir gennych i ddarparu a derbyn ffurflenni cais ar-lein ar gyfer darpar-gyfranwyr, neu gwmni sy'n darparu ffurflenni rhyddhau cyfranwyr ar-lein, y gellir eu llofnodi ar leoliad ar iPad.

Dylai eich contract gyda'r cwmnïau hynny gynnwys:

- hyd y cyfnod prosesu;
- natur a diben y prosesu; y categorïau o ddata personol a phynciau'r data;
- eich hawliau a'ch rhwymedigaethau chi fel rheolydd data;
- mai data fel y cyfarwyddir gennych chi, yn unig, a brosesir gan y prosesydd data;
- bod rhaid i'r prosesydd data sicrhau y gosodir rhwymedigaethau cyfrinachedd priodol ar y personau a awdurdodir ganddo i brosesu data personol;
- bod y prosesydd data wedi sefydlu'r mesurau diogelwch gofynnol;
- na chaiff y prosesydd data is-gontractio i brosesydd data arall heb eich caniatâd penodol chi, ac os bydd is-gontractio, y gosodir yr un rhwymedigaethau ar yr is-gontractwr;
- y bydd y prosesydd data yn eich cynorthwyo i gymryd camau technegol a threfniadol priodol er mwyn cyflawni eich rhwymedigaethau i wrthrychau'r data;
- y bydd y prosesydd data yn eich cynorthwyo i gydymffurfio â'ch rhwymedigaethau o dan Erthyglau 32 i 36 o'r GDPR; ac y bydd y prosesydd data yn eich hysbysu ynghylch unrhyw dor diogelwch data;
- y bydd y prosesydd data yn dileu neu'n dychwelyd yr holl ddata personol ar ddiwedd cyfnod darparu'r gwasanaethau, ac y caniateir i chi gynnal archwiliad o'r prosesydd data i gael cadarnhad o'i gydymffurfiaeth.

Rhaid i chi sicrhau bod eich prosesydd data yn ymrwymo i gydymffurfio â'r GDPR. Byddwch chi, fel y rheolydd data, yn gyfrifol am unrhyw doriadau o'r GDPR a fydd yn deillio o weithgareddau a gyflawnir gan y prosesydd data ar eich rhan chi. Fodd bynnag, bydd prosesydd data hefyd yn gyfrifol am unrhyw fethiant ganddo i gydymffurfio â'i rwymedigaethau GDPR. Os daw toriad diogelwch data i sylw'r prosesydd data, rhaid iddo eich hysbysu chi ynghylch hynny heb oedi.

Yn ogystal, mae gan broseswyr data gyfrifoldebau uniongyrchol o dan y GDPR, a gallant gael eu dirwyo neu ddioddef sancsiynau eraill os nad ydynt yn cydymffurfio.

Er enghraifft, os bydd prosesydd data yn defnyddio is-gontractwr, bydd y prosesydd data gwreiddiol yn parhau'n uniongyrchol atebol i'r rheolydd data am gyflawni rhwymedigaethau'r is-gontractwr. Yn ychwanegol at ei rwymedigaethau contractiol i'r rheolydd data, mae gan brosesydd data y cyfrifoldebau uniongyrchol canlynol o dan y GDPR:

- peidio â defnyddio is-gontractwr heb gel awdurdodiad ysgrifenedig ymlaen llaw gan y rheolydd data;
- cydweithredu â'r awdurdodau goruchwyliol (megis Swyddfa'r Comisiynydd Gwybodaeth);
- sicrhau diogelwch ei brosesu;
- cadw cofnod o'i weithgareddau prosesu;
- hysbysu'r rheolydd data ynghylch unrhyw doriadau data personol;
- cyflogi swyddog diogelu data (pan fo angen).

O dan y GDPR mae'n ofynnol eich bod chi, sef y rheolydd data, wedi sefydlu contract gyda'ch prosesydd data a fydd yn pennu telerau fel y nodir uchod.

Os yw prosesydd data yn peidio â bodloni unrhyw un o'r rhwymedigaethau hyn neu'n gweithredu y tu allan, neu'n groes, i gyfarwyddiadau'r rheolydd data neu'r hyn sy'n ofynnol ganddo o dan y GDPR, yna, yn dilyn achos cyfreithiol gall fod yn atebol i dalu iawndal, neu ddirwyo, neu ddioddef cosbau neu fesurau unioni eraill a bennir gan Swyddfa'r Comisiynydd Gwybodaeth.

Pan fo prosesydd data yn prosesu data personol a allai, pe byddid yn eu colli, eu difrodi neu'u datgelu heb awdurdod priodol, achosi niwed i unigolion, i'ch cwmni neu i'r darlledwr sy'n eich comisiynu yng nghyd-destun cynhyrchiad, mae'n briodol: (i) darparu'n benodol yn eich contract gyda'ch prosesydd data fod rhaid i'r prosesydd data gydymffurfio â gofynion y GDPR; (ii) cynnwys darpariaeth yn y contract i'ch galluogi i archwilio a/neu fonitro cydymffurfiaeth y prosesydd data pan fo hynny'n ymarferol ac angenrheidiol, a bod rhaid i'r prosesydd data sicrhau bod yr holl wybodaeth y mae ei hangen ar gael i chi, er mwyn dangos ei fod yn cydymffurfio.

Mae rhagor o wybodaeth ar gael gan Swyddfa'r Comisiynydd Gwybodaeth am ystyron data personol, rheolwyr data a phroseswyr data: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.

8. Egwyddorion y GDPR – Polisïau a Phersonol

Rhaid i bob cwmni cynhyrchu fod wedi sefydlu polisi diogelu data priodol neu bolisi diogelwch data cyfwerth sy'n pennu'r modd y byddant yn rheoli data personol, o fewn y cwmni ac wrth wneud rhaglenni. Dylai'r polisi ymgorffori **Egwyddorion y GDPR**. Mae'r egwyddorion hyn yn debyg i'r rheini yn y DDD 1998, ynghyd â gofyniad atebolrwydd newydd i'r perwyl bod rheolydd data yn gyfrifol am gydymffurfio, a bod rhaid iddo allu arddangos ei fod yn cydymffurfio, â'r egwyddorion.

Rhaid i bob cwmni sicrhau bod data personol:

i. yn cael eu prosesu yn gyfreithlon, yn deg ac mewn modd tryloyw.

ii. yn cael eu casglu at ddibenion, penodol, penodedig sy'n ddilys a chyfreithlon (ystyrir bod prosesu pellach ar gyfer archifo, dibenion sydd er budd y cyhoedd, ymchwil wyddonol neu hanesyddol, neu ddibenion ystadegol yn anghydnaws â'r dibenion gwreiddiol) ;

iii. yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol;

iv. yn fanwl gywir, a phan fo angen, yn cael eu diweddaru'n gyson; rhaid cymryd pob cam rhesymol i sicrhau bod data personol sy'n anghywir, gan ystyried at ba ddibenion y'u prosesir, yn cael eu dileu neu'u hunioni yn ddi-oed;

v. yn cael eu cadw mewn ffurf a fyddai'n caniatáu adnabod gwrthrychau'r data am ddim hwy nag sy'n angenrheidiol at y dibenion (ni cheir gwneud hyn am gyfnodau hwy ac eithrio ar gyfer archifo er budd y cyhoedd, ymchwil wyddonol neu hanesyddol, neu ddibenion ystadegol yn unig– a hynny ar yr amod y gweithredir mesurau technegol priodol i ddiogelu hawliau a rhyddid unigolion);

vi. yn cael eu diogelu yn briodol, gan gynnwys eu diogelu rhag eu prosesu yn anghyfreithlon neu heb awdurdod, a rhag eu colli, eu dinistrio neu'u difrodi yn ddamweiniol, trwy weithredu mesurau technegol neu drefniadol priodol.

9. Beth yw sail gyfreithlon o dan y GDPR?

Er mwyn prosesu data o dan y GDPR bydd rhaid i chi fod â sail gyfreithlon. Mae Swyddfa'r Comisiynydd Gwybodaeth yn argymell y dylech gadw cofnod o'r sail gyfreithlon y byddwch yn dibynnu arni ar gyfer pob gweithgaredd prosesu, ynghyd ag esboniad pam y mae'r sail honno yn berthnasol. Dylech roi gwybod i wrthrychau'r data beth yw eich sail gyfreithlon, yn rhan o'ch hysbysiad preifatrwydd a/neu'ch polisi preifatrwydd, ar yr adeg y byddwch yn casglu'r data personol.

Mae egwyddor gyntaf y GDPR yn ei gwneud yn ofynnol i brosesu pob data personol yn gyfreithlon, yn deg ac mewn modd tryloyw. Pan nad oes sail gyfreithlon i'r prosesu, bydd y prosesu yn anghyfreithlon ac yn torri'r egwyddor gyntaf.

Dylech adolygu'r sail sydd i'r modd yr ydych yn prosesu data personol o dan y GDPR, gan ei chymharu â'r sail flaenorol o dan y DDD 1998. Dichon y byddwch yn penderfynu bod sail wahanol yn fwy priodol o dan GDPR (gweler adran 10). Os oes sail gyfreithlon ar gyfer prosesu at ddiben newydd bydd angen i chi, er hynny, ystyried a yw prosesu at y diben newydd yn deg a thryloyw.

Rhoddir canllawiau gan Swyddfa'r Comisiynydd Gwybodaeth yn: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Mae Swyddfa'r Comisiynydd Gwybodaeth wedi darparu offeryn rhyngweithiol i'ch helpu i ganfod y sail gyfreithlon berthnasol:
https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/

10. Seiliau cyfreithlon sy'n caniatáu i chi drin data personol.

Mae chwech o seiliau cyfreithlon y gellir dewis o'u plith. Bydd pob un o'r seiliau cyfreithlon yn effeithio ar hawliau'r unigolyn. Ac eithrio mewn perthynas â chydsyniad, cewch weithredu ar fwy nag un sail gyfreithlon; ac os gwnewch hynny, dylech nodi a dogfennu pob un o'r seiliau y gweithredir arnynt mor fuan ac y bo modd. Os byddwch yn gweithredu ar y sail gyfreithlon o gydsyniad, gall hynny achosi canlyniadau difrifol wrth wneud rhaglenni. Dylech geisio cyngor cyfreithiol ynglŷn ag a ddylech ddibynnu ar gydsyniad fel sail gyfreithlon ar gyfer eich rhaglen.

Rhestrir ac esbonnir y chwe sail gyfreithlon isod:

10.1 Cydsyniad

Bellach, o dan y GDPR, mae'n sylweddol anos cael cydsyniad dilys, ac felly, yn aml iawn nid hon yw'r sail gyfreithlon orau i ddibynnu arni ar gyfer prosesu data personol unigolyn. Mae'n bwysig nodi na all cydsyniad unigolyn i brosesu ei ddata personol fod yn amodol, e.e ar ei ymddangosiad mewn rhaglen. Rhaid rhoi'r cydsyniad yn rhydd o amodau, a rhaid i'r unigolyn feddu'r hawl i dynnu'r cydsyniad yn ôl ar unrhyw adeg. Er mwyn gall prosesu data ar y sail gyfreithlon hon:

- rhaid i unigolyn fod wedi rhoi cydsyniad **eglur** a diamwys i chi, i brosesu ei ddata personol at y diben penodol y gofynnwyd am y cydsyniad ar ei gyfer.
- mae'n ofynnol bod yr unigolyn yn optio i mewn yn gadarnhaol/dylech allu dangos yn eglur sut y bu i'r unigolyn gymryd cam cadarnhaol i ddynodi ei fod yn cydsynio; ac
- mae angen i'r unigolyn allu tynnu'n ôl ei gydsyniad ar unrhyw adeg (a rhaid i chi roi gwybod i'r unigolyn sut y gall dynnu ei gydsyniad yn ôl). Dylai fod cyn hawsed i'r unigolyn dynnu ei gydsyniad yn ôl ag yr oedd iddo roi ei gydsyniad ar y dechrau.

Byddech yn dibynnu ar gydsyniad fel sail ar gyfer prosesu wrth farchnata i unigolyn, a dylech felly ymgyfarwyddo â'r gofynion marchnata uniongyrchol yn Rheoliadau Preifatrwydd a Chyfathrebu Electronig 2003.

Darllenwch y canllawiau ar y Rheoliadau Preifatrwydd a Chyfathrebu Electronig gan Swyddfa'r Comisiynydd Gwybodaeth yn: https://ico.org.uk/for-organisations/guide-to-pecr/

Nodyn i Gynhyrchwyr:
Gan amlaf, nid Cydsyniad fydd y sail gyfreithlon fwyaf priodol ar gyfer prosesu mewn perthynas â rhaglen, oherwydd y gofyniad y gall person dynnu yn ôl ei gydsyniad ar unrhyw adeg, a byddai tynnu cydsyniad yn ôl felly yn cael effaith sylweddol ar eich gallu chi i gyflenwi eich rhaglen i ddarlledwr. Felly, os oes modd, ni ddylech ddibynnu ar gydsyniad fel sail gyfreithiol ar gyfer eich prosesu; ond os yw'r amgylchiadau yn ansicr, a hwyrach yn peri y bydd angen dibynnu ar gydsyniad, dylech geisio cyngor cyfreithiol.

- Fel arfer mae casglu a phrosesu data personol cyfranwyr yn angenrheidiol at y diben o gyflawni'r contract cyfranwyr (gweler adran 10.2 isod). Ystyriwch yn ofalus, yng ngoleuni'r gallu i dynnu cydsyniad yn ôl yn rhwydd, a fyddai'n briodol a/neu'n ddoeth dibynnu ar gydsyniad (neu ddibynnu ar gydsyniad pan fo hynny'n gwbl angenrheidiol, gan wneud yn eglur pa bryd na ellir tynnu'r cydsyniad yn ôl, er enghraifft, wedi i wybodaeth gael ei datgelu i'r cyhoedd oherwydd cyfranogiad y cyfrannwr).

- Mae'n bwysig gwahaniaethu rhwng cydsyniad ar gyfer prosesu data personol a'r gofyniad i sicrhau cydsyniad ar sail gwybodaeth i gymryd rhan mewn rhaglen, fel y'i pennir yng Nghod Darlledu Ofcom, ac a fydd yn parhau'n ofynnol.

10.2 Contract

Mae "anghenraid contractiol" yn parhau'n sail gyfreithlon ar gyfer prosesu data personol data fel yr oedd gynt o dan y DDD 1998. Gellwch ddefnyddio cydymffurfiaeth â chontract yn sail gyfreithlon os yw'ch prosesu yn angenrheidiol ar gyfer cyflawni contract y mae'r unigolyn yn barti ynddo, neu cyn ymuno mewn contract os oes perthynas gontractiol yn

yr arfaeth. Bydd angen i chi sicrhau bod y prosesu yn angenrheidiol, eich bod wedi dogfennu eich penderfyniad i ddefnyddio'r sail gyfreithlon hon, a bod y partïon wedi cytuno y cewch ddefnyddio'r sail gyfreithlon hon ar gyfer prosesu.

Nodyn i Gynhyrchwyr:
Dylech sicrhau bod unigolion sy'n ymdrin â gwneud rhaglenni, neu'n cyfrannu i'r gwaith hwnnw, wedi eu contractio o dan gytundeb/contract a'u bod yn gwybod mai ar y sail gyfreithlon honno y prosesir eu data personol wrth wneud y rhaglen. Byddai'n ddoeth hefyd cael sail gyfreithiol ychwanegol y gellir dibynnu arni yn y cytundeb cyfranwr/ffurflen ryddhau, megis buddiant dilys.

10.3 Cydymffurfiaeth/ rhwymedigaeth gyfreithiol

Enghraifft o brosesu i gydymffurfio â rhwymedigaeth gyfreithiol fyddai prosesu manylion banc rhywun ac yna dal gafael arnynt i gydymffurfio â rheolau CThEM, neu brosesu gwybodaeth am alergedd bwyd cyfrannwr i sioe goginio er mwyn cydymffurfio â'n rhwymedigaethau Iechyd a Diogelwch. Y prif newid o dan y sail gyfreithlon hon, o gymharu â'r DDD 1998, yw bod GDPR yn benodol yn cyfyngu'r rhwymedigaethau cyfreithiol hyn i rai sy'n codi o dan gyfraith y Deyrnas Unedig neu'r Undeb Ewropeaidd. Gallai hyn beri bod sefydliad sy'n ddarostyngedig i orchymyn llys o'r tu allan i'r Undeb Ewropeaidd eich gosod mewn sefyllfa anodd.

10.4 Buddiannau allweddol gwrthrych y data

Gellwch ddibynnu ar y categori hwn os byddwch yn prosesu data personol rhywun er mwyn diogelu ei fywyd, a phan fo'r prosesu yn ymwneud ag iechyd neu ddata categori arbennig a hynny, yn unig, mewn sefyllfaoedd pan na ellir rhoi cydsyniad. Er enghraifft, pan fo angen gofal iechyd ar frys ar unigolyn mewn ysbyty, ac nad yw ei gyflwr yn ei alluogi i roi cydsyniad i brosesu ei ddata.

10.5 Cyflawni tasg er lles y cyhoedd

Prosesu sy'n angenrheidiol er mwyn cyflawni tasg sydd er lles y cyhoedd neu gyflawni swyddogaeth gyhoeddus, pan fo sail eglur mewn cyfraith i'r dasg neu'r swyddogaeth honno.

10.6 Buddiant dilys

Hon yw'r fwyaf hyblyg o'r seiliau sydd ar gael, sef prosesu a gyflawnir ar y sail ei fod "er buddiannau dilys" y rheolydd data neu eraill. Mae'r sail hon yn fwyaf priodol pan ddefnyddir data unigolion yn y ffyrdd y byddai'r unigolion yn disgwyl yn rhesymol i'r data gael eu defnyddio, ac na fyddai'r prosesu'n cael effaith arnynt na ellir ei chyfiawnhau, o'i wrthbwyso yn erbyn buddiannau, hawliau a rhyddid yr unigolion. Wrth brosesu data personol ar y sail hon, bydd angen i chi gymryd gofal a derbyn cyfrifoldeb ychwanegol am ystyried a diogelu hawliau a buddiannau pobl, a dogfennu eich asesiad o'r buddiannau dilys. Gall buddiannau dilys olygu eich buddiant chi neu fuddiant trydydd partïon. Gallant gynnwys buddiant masnachol, buddiant unigolyn neu fuddion cymdeithasol ehangach. Fodd bynnag, os dewiswch ddibynnu ar fuddiant dilys, byddwch yn ymgymryd â chyfrifoldeb ychwanegol am ystyried a diogelu hawliau a buddiannau pobl. Bydd angen i chi hefyd gynnwys manylion am eich buddiant dilys yn eich gwybodaeth breifatrwydd. Yn ymarferol, fodd bynnag, mae'n debygol y bydd anghenraid gontractiol a'r angen i gydymffurfio â rhwymedigaeth gyfreithiol yn seiliau cyfreithlon mwy addas.

I gael rhagor o wybodaeth, darllenwch ganllawiau Swyddfa'r Comisiynydd Gwybodaeth ar fuddiannau dilys:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Nodyn i Gynhyrchwyr:
Rhaid i gynhyrchydd bennu ei sail gyfreithlon cyn prosesu data personol. Mae hyn yn golygu y dylech bennu eich sail gyfreithlon cyn dechrau gwneud rhaglen, neu os nad yw hynny'n bosibl, dylech wneud hynny mor gynnar ac y bo modd. Rhaid dogfennu eich sail gyfreithlon, ynghyd â'r rheswm pam y dewiswyd y sail honno. Yn dibynnu ar y math o raglen yr ydych yn ei ffilmio, hwyrach y byddwch yn dewis trafod eich sail gyfreithlon gyda'r darlledwr sy'n eich comisiynu, oherwydd gall fod mwy nag un sail gyfreithlon, er enghraifft:

- Pennu eich sail gyfreithlon wrth gynnwys neu gontractio pobl a fydd ffilmio gyda chi yn eich rhaglen, h.y. mae'n debygol mai cyflawni contract fydd hyn. Pe byddech yn dibynnu ar gydsyniad, gallai person dynnu ei gydsyniad yn

ôl ar unrhyw adeg, a byddai hynny'n cael effaith sylweddol ar eich gallu i gyflenwi eich rhaglen i ddarlledwr. Gweler pwynt 10.1 am ragor o wybodaeth ynghylch hyn.

- Hysbysiadau Ffilmio Cyhoeddus: byddai hyn yn debygol o fod yn ddarostyngedig i'r sail gyfreithlon o fuddiant dilys.
- Ffilmio dirgel: byddai hyn yn debygol o ddibynnu ar y sail gyfreithlon o fuddiant dilys neu esemptiad newyddiadurol

11 Yr amodau prosesu sy'n caniatáu i chi drin data categori arbennig

Gan fod data categori arbennig yn fwy sensitif o ran eu natur, mae angen gwneud rhagor i'w diogelu. Gallai'r math hwn o ddata greu risgiau sylweddol i hawliau a rhyddid unigolyn, er enghraifft, risg o wahaniaethu'n anghyfreithlon yn ei erbyn, pe digwyddai toriad diogelwch neu pe prosesid y data yn anghywir.

Mae'r GDPR wedi darparu seiliau ychwanegol y gellir prosesu'r wybodaeth hon yn gyfreithlon oddi tanynt. Er mwyn prosesu data categori arbennig rhaid i chi nodi amod ar wahân yn ogystal â sail gyfreithlon; pennir yr amodau hyn yn Rhan 2, Pennod 2, para 10 o'r DDD 2018 ac Atodlen 1 i'r Ddeddf honno.

11.1 **Caniatâd penodol:** pan fo person wedi rhoi caniatâd penodol i ddefnyddio'r wybodaeth, er mwyn dilysu'r prosesu. Sylwch fod rhai o'r amodau eraill hefyd yn gwneud yn ofynnol eich bod yn ystyried cael caniatâd penodol yn gyntaf, neu'n cael caniatâd ar gyfer rhai elfennau o'ch prosesu. Er enghraifft, os ydych yn gorff dielw ac yn dewis dibynnu ar Erthygl 9(2)(d), bydd yn dal yn ofynnol cael caniatâd penodol er mwyn datgelu'r data i unrhyw reolwyr trydydd-parti.

Os gwelwch yn dda, darllenwch ganllawiau Swyddfa'r Comisiynydd Gwybodaeth ar ganiatâd penodol: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

11.2 **Cyfraith cyflogaeth:** sef gweithredu rhwymedigaethau a hawliau ar gyfer cyflogaeth, nawdd cymdeithasol, cyfraith amddiffyniadau cymdeithasol, neu gydgytundeb;

11.3 **Buddiannau allweddol**: sy'n diogelu'r person pan nad oes ganddo'r gallu corfforol neu gyfreithiol, i roi ei ganiatâd. Y bwriad yw gweithredu hyn mewn sefyllfaoedd 'bywyd neu farwolaeth' pan fo angen gofal iechyd ar rywun ar frys mewn argyfwng;

11.4 **Elusennau neu gyrff dielw:** pan fo gan sefydliad, cymdeithas, neu gorff dielw arall, nod gwleidyddol, athronyddol neu grefyddol, neu os yw'n undeb llafur, ar yr amod bod y corff yn ymwneud yn unig ag aelodau neu gyn-aelodau'r corff, neu bersonau sydd mewn cysylltiad rheolaidd â'r corff, ac na ddatgelir data personol y tu allan i'r corff hwnnw heb ganiatâd y person dan sylw;

11.5 **Data a ddatgelwyd yn gyhoeddus gan wrthrych y data**: gwybodaeth bersonol sydd wedi ei datgelu yn agored i'r cyhoedd gan yr unigolyn ei hunan. Gall hyn fod yn berthnasol pan gynhwysir data categori arbennig yn olygyddol mewn rhaglen.

11.6 **Hawliadau cyfreithiol:** pan wneir neu pan amddiffynnir hawliadau cyfreithiol, neu pan fo llys yn cyflawni ei swyddogaeth farnwrol;

11.7 **Budd cyhoeddus sylweddol:** pan fo rhesymau o fudd sylweddol i'r cyhoedd. Mae Atodlen 1 i'r DDD 2018 yn rhestru nifer o amodau sy'n bodloni'r gofyniad o fudd cyhoeddus sylweddol, megis rhwymedigaeth o dan gyfraith Iechyd a Diogelwch. Bydd angen i chi fodloni o leiaf un o'r amodau yn Atodlen 1. Rhaid i hyn fod yn gymesur â'r nod y ceisir ei gyrraedd a pharchu'r hawl i ddiogelu data, ac ar yr un pryd ddarparu mesurau addas a phenodol i ddiogelu hawliau sylfaenol a buddiannau'r person sydd o dan sylw.

11.8 **Diagnoses a thriniaethau meddygol:** ar gyfer meddygaeth ataliol/alwedigaethol, ar gyfer asesu gallu cyflogai i weithio, diagnosis meddygol, darparu gofal neu driniaeth iechyd neu ofal cymdeithasol neu reolaeth systemau iechyd neu ofal cymdeithasol neu ar gyfer contractio gyda gweithiwr proffesiynol iechyd.

11.9 **Iechyd y cyhoedd:** megis diogelu rhag bygythiadau trawsffiniol difrifol i iechyd y cyhoedd, sicrhau safonau uchel o ran ansawdd a diogelwch gofal iechyd/cynhyrchion meddyginiaethol neu ddyfeisiau meddygol, gan sicrhau y diogelir hawliau'r unigolyn a chyfrinachedd proffesiynol;

11.10 **Hanesyddol, Ystadegol neu Wyddonol:** ar gyfer archifo at ddibenion budd y cyhoedd, ymchwil wyddonol neu hanesyddol, neu ddibenion ystadegol, yn gymesur â'r nod y ceisir ei gyrraedd.

Nodyn i Gynhyrchwyr:
Mae cynhyrchwyr yn debygol o ddibynnu ar nifer o'r amodau uchod ochr yn ochr â sail gyfreithlon megis anghenraid gontractiol a/neu fuddiant dilys. Rhaid i chi bennu un o'r amodau uchod yn ogystal â sail gyfreithlon er mwyn prosesu data categori arbennig. Er enghraifft, gellwch ddefnyddio data categori arbennig mewn amgylchiadau fel a ganlyn:

- i gasglu gwybodaeth at ddibenion cyflogaeth, neu ddefnyddio cyd-drefniadau i dalu gweddilldaliadau/ breindaliadau;
- ar gyfer rhaglenni, cewch gynnwys data categori arbennig a ddatgelwyd yn agored i'r cyhoedd eisoes gan y person sydd dan sylw ei hunan;
- i gynnal asesiadau meddygol er mwyn deall galluoedd y cyflogai/gweithiwr/unigolyn, er enghraifft cynnal profion seicolegol ar gyfranwyr ac eraill;
- at ddibenion hanesyddol wrth wneud rhaglenni sy'n creu ac yn archifo gwybodaeth sydd er budd y cyhoedd; ac
- yn olaf, pan fo'ch prosesu er budd sylweddol i'r cyhoedd, ar yr amod bod y data categori arbennig a ddefnyddir gennych yn deg a chymesur ac y gweithredir mesurau i ddiogelu hawliau'r unigolion perthnasol.

12. Sail gyfreithlon sy'n caniatáu i Gynhyrchydd drin data plant

Mae angen cymryd gofal penodol wrth drin data plant o dan y GDPR.

Cewch ddefnyddio unrhyw un o'r seiliau cyfreithlon a bennir yn y GDPR wrth brosesu data personol plant. Dylai tegwch fod yn ystyriaeth ganolog bob amser wrth brosesu data plant, ond yn achos rhai o'r seiliau, mae rhai materion ychwanegol y dylech feddwl amdanynt os yw gwrthrych y data yn berson ifanc o dan 13 oed, er enghraifft, pa un a oes arnoch angen caniatâd rhiant neu warcheidwad.

- **Cydsyniad**: Os eich bwriad yw dibynnu ar gydsyniad y plentyn fel eich sail gyfreithlon ar gyfer prosesu, rhaid i chi sicrhau bod y plentyn yn ddigon hen i ddeall i beth y mae'n cydsynio; oni sicrheir hynny, gall y cydsyniad fod yn annilys gan nad yw 'ar sail gwybodaeth'. Cyfrifoldeb y Rheolydd yw gwirio pwy ddylai roi cydsyniad. Mae yna hefyd rai rheolau ychwanegol ar gyfer cydsynio ar-lein; ac yn achos plentyn o dan 13 mlwydd oed, bydd angen cydsyniad rhiant neu warcheidwad cyfreithiol. Dylech fod yn ymwybodol o'r goblygiadau a all godi os dibynnir ar gydsyniad fel sail ar gyfer prosesu. Rhoddir gwybodaeth bellach am hyn yn 10.1 uchod ac ar wefannau Swyddfa'r Comisiynydd Gwybodaeth.

- **Contract**: Os eich bwriad yw dibynnu ar 'gyflawni contract' fel eich sail gyfreithlon ar gyfer prosesu, bydd rhaid i chi ystyried a yw'r plentyn yn gymwys i gytuno i'r contract ac i ddeall goblygiadau'r prosesu, a gofyn am gydsyniad rhiant neu warcheidwad pan fo'n briodol. Mae'n bwysig nodi bod Cod Darlledu Ofcom yn cyfeirio at blant fel unrhyw rai sydd o dan 18 oed.

  Ceir rhagor o wybodaeth gan Ofcom am ddiogelu rhai o dan 18 oed yn: https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-one-protecting-under-eighteens

- **Buddiannau dilys:** Os eich bwriad yw dibynnu ar fuddiannau dilys fel eich sail gyfreithlon ar gyfer prosesu, bydd rhaid i chi, wrth brosesu'r data personol, wrthbwyso eich buddiannau dilys chi eich hun (neu fuddiannau trydydd parti) yn erbyn buddiannau, hawliau sylfaenol a rhyddid y plentyn. Mae hyn yn golygu paratoi asesiad a dyfarniad ysgrifenedig ynglŷn â natur a phwrpas y prosesu, a'r risgiau posibl y mae'n ei achosi i blant. Mae'n ofynnol hefyd eich bod yn cymryd camau priodol i ddiogelu rhag y risgiau hynny.

Mae canllawiau pellach ar gael gan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

13. Casglu data personol – Hysbysiad Preifatrwydd

Datganiad yw hysbysiad preifatrwydd, sy'n dweud wrth unigolyn pwy sy'n casglu ei wybodaeth bersonol ac at ba ddiben y caiff yr wybodaeth honno ei defnyddio, ac yn rhoi manylion am unrhyw drydydd partïon y bwriedir rhannu'r data personol gyda hwy, yn rhan o'r prosiect neu wrth wneud y rhaglen. Mae'r GDPR yn gwneud yn ofynnol bod rheolydd data yn darparu rhagor o wybodaeth am y modd y bwriedir prosesu data personol ar yr adeg y'u cesglir; a'r drefn orau yn aml fydd cynnwys yr wybodaeth honno yn y datganiad preifatrwydd.

Mae ffurf yr hysbysiad preifatrwydd yn amrywio; gall fod yn hysbysiad ar wefan neu'n sgript a ddarllenir ar lafar dros y teleffon. Rhaid iddo fod yn gryno ac eglur ac ar gael yn hwylus i'r unigolion, a dylech ddogfennu'r modd y rhoddwyd yr hysbysiad a pha bryd y gwnaed hynny. Dylid bod yn arbennig o ofalus i amddiffyn plant wrth gasglu a phrosesu eu data personol, gan y gallent fod yn llai ymwybodol o'r risgiau sy'n gysylltiedig

Dywed y GDPR fod rhaid i'r wybodaeth a ddarperir gennych:

- fod yn gryno, tryloyw, dealladwy a hygyrch;
- fod wedi ei hysgrifennu mewn iaith eglur a phlaen, yn enwedig os anelir hi at blentyn;
- fod ar gael yn ddi-dâl;
- nodi at ba ddiben y bwriedir prosesu'r data personol; and
- nodi'r sail gyfreithlon ar gyfer prosesu.

Dylai hysbysiad preifatrwydd fod yn hysbysiad penodol ar gyfer y prosiect neu'r rhaglen a baratoir. Dylai fod yn wahanol ac ar wahân i bolisi diogelu data'r cwmni, sy'n ddogfen yn manylu mwy am y modd y mae'ch cwmni yn casglu ac yn prosesu data personol, hawliau gwrthrychau'r data, ac amcanion a chyfrifoldebau'r cwmni mewn perthynas â data personol.

14. <u>Pa wybodaeth y mae angen i chi ei darparu yn yr hysbysiad preifatrwydd?</u>

Pwy ydych chi: Manylion am y cwmni, ac unrhyw gyrff cysylltiol a fydd yn cydweithio gyda chi ar y prosiect/rhaglen.

Pwy yw eich Swyddog Diogelu Data/Rheolwr Data/ Uwch-gynghorydd Data: (os oes gennych un) neu arweinydd, neu fanylion cyswllt cyffredinol.

Pa ddata y byddwch yn eu casglu a'u prosesu yn y rhaglen/prosiect: Rhestrwch yr wybodaeth bersonol y byddwch yn ei chasglu a'i phrosesu a'r rhesymau dros brosesu. A oes mwy nag un rheolydd?

Y sail gyfreithlon dros ddefnyddio data: Y sail gyfreithlon ar gyfer prosesu, beth y bwriedwch ei wneud gyda'r data a pha bryd y byddwch/na fyddwch yn eu prosesu.

Os ydych yn dibynnu ar gydsyniad fel sail gyfreithlon. Dylech arddangos hynny yn eglur ac amlwg. Dylid gofyn i unigolion optio i mewn trwy gymryd camau positif, crybwyll bod hawl gan unigolyn i dynnu ei gydsyniad yn ôl ac esbonio sut y gall wneud hynny. Dylai fod blwch optio ar wahân heb dic ynddo ar gyfer marchnata uniongyrchol.

Rhannu data: Gyda phwy y byddwch yn rhannu data personol a pham? Er enghraifft, os oes posibilrwydd y byddwch yn rhannu adroddiadau seicolegol gyda'ch darlledwr, dylech ddatgan hynny yma. Byddai'n arfer da ychwanegu dolen gyswllt i'ch polisi preifatrwydd, a dylai'r polisi hwnnw esbonio gyda phwy y byddwch yn rhannu data.

Buddiannau dilys: Os eich bwriad yw dibynnu ar fuddiannau dilys fel y sail gyfreithlon ar gyfer prosesu, bydd angen i chi nodi pa fuddiannau dilys sy'n berthnasol, a chymryd i ystyriaeth y prawf gwrthbwyso.

Data personol a drosglwyddir y tu allan i'r Ardal Economaidd Ewropeaidd: Os byddwch yn trosglwyddo data personol i rywle y tu allan i'r AEE, bydd angen rhoi ystyriaeth i'r rhagofalon y dylid eu gweithredu.

Gwybodaeth ychwanegol y bydd angen i chi ei chymryd i ystyriaeth: am ba gyfnod y cedwir y data; at bwy yr eir i gael gwybodaeth am hawliau gwrthrychau'r data (hynny yw, y polisi preifatrwydd); yr hawl i gwyno wrth Swyddfa'r Comisiynydd Gwybodaeth; a gwybodaeth am wneud penderfyniadau awtomataidd.

Hysbysiadau preifatrwydd ar gyfer grwpiau sy'n agored i niwed: Os byddwch yn casglu gwybodaeth gan unigolion sy'n agored i niwed megis plant, rhaid i chi sicrhau y trinnir yr unigolion hynny yn deg. Dylid drafftio hysbysiadau preifatrwydd sy'n briodol ar gyfer lefel dealltwriaeth y gynulleidfa a dargedir; hynny yw, defnyddio iaith sy'n briodol i'w hoedran. Cyflwynwch yr wybodaeth breifatrwydd mewn ffyrdd sy'n gyfeillgar i blant, gan ddefnyddio diagramau, cartwnau, graffigion, dangosfyrddau, hysbysiadau haenog neu union-adeg, iconau a symbolau, gan ystyried oedran y plentyn hefyd, ac a oes angen darparu'r un wybodaeth i riant, gwarcheidwad neu ofalwr y plentyn.

Hysbysiadau preifatrwydd i bobl nad Cymraeg na Saesneg yw eu mamiaith: Os byddwch yn casglu gwybodaeth gan bobl nad yw Cymraeg na Saesneg yn famiaith iddynt, dylech ystyried a ddylid darparu eich hysbysiadau preifatrwydd mewn iaith arall, er nad oes rhwymedigaeth gyfreithiol arnoch i gynnig cyfieithiadau.

Cydsyniad plentyn ar gyfer gwasanaeth ar-lein: Mae caniatâd rhiant yn ofynnol ar gyfer prosesu data personol plentyn (o dan y GDPR, plentyn yw unrhyw un sydd o dan 16 oed). Mewn rhai cyd-destunau (yn enwedig ar-lein), gall fod yn anodd profi bod caniatâd rhiant neu warcheidwad cyfreithiol wedi ei sicrhau. Os byddwch yn cynnig gwasanaeth ar-lein yn uniongyrchol i blant ac yn dibynnu ar gydsyniad fel eich sail gyfreithlon ar gyfer prosesu data personol, plant sy'n 13 oed neu'n hŷn, yn unig, a fydd â'r gallu i gydsynio drostynt eu hunain yn y DU o dan y DDD 2018; ar gyfer plant sydd o dan 13 oed, bydd caniatâd rhiant neu warcheidwad cyfreithiol yn ofynnol. Os byddwch yn targedu'r marchnadoedd Ewropeaidd ehangach, rhaid sicrhau eich bod yn cydymffurfio â pha bynnag derfynau oedran sydd mewn grym ym mhob Aelod-wladwriaeth. Er enghraifft, yn Ffrainc a'r Almaen, yr oedran cydsynio ar-lein yw 16 (mae'r terfyn oedran perthnasol wedi ei bennu yn neddfwriaeth pob un o'r Aelod-wladwriaethau sy'n gweithredu'r GDPR).

Gweler y canllawiau cysylltiedig gan Swyddfa'r Comisiynydd Gwybodaeth:

- Buddiant dilys: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/
- Trosglwyddiadau i'r tu allan i AEE : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/
- Atebolrwydd a llywodraethu: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/
- Yr hawl i gael gwybod: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
- Proffilio awtomataidd: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

15. Hawliau unigolion a'r hyn y dylid ei ystyried wrth ddrafftio eich polisi preifatrwydd

Mae' GDPR yn sefydlu wyth o hawliau penodol ar gyfer gwrthrych y data, a bydd angen i chi ddangos eich bod yn cydymffurfio trwy ymgorffori'r hawliau hynny yn y modd y byddwch yn prosesu data. Mae gan blant yr un hawliau dros eu data personol ag y sydd gan oedolion. Rhoddir manylion pellach isod am yr hawliau hyn sydd yn y GDPR.

15.1 Hawl i gael gwybod:

Mae gan unigolion yr hawl i gael gwybod am y modd y defnyddir eu data personol, a dylid rhoi'r wybodaeth iddynt ar yr adeg y byddwch yn casglu'r data personol ganddynt. Os byddwch yn cael data personol o ffynonellau eraill, rhaid i chi ddarparu gwybodaeth breifatrwydd i'r unigolion ar yr adeg y cyfathrebwch gyntaf gyda gwrthrych y data, neu pan ddatgelir data personol gyntaf i dderbynnydd arall. Fodd bynnag, rhaid gwneud hyn **ddim hwyrach nag un mis** ar ôl cael y data.

Plant: Mae gan blant yr un hawliau ag ysydd gan oedolion dros eu data personol a chânt arfer eu hawliau eu hunain cyn belled â'u bod yn gymwys i wneud hynny. Pan nad ystyrir bod y plentyn ei hunan yn gymwys, gall oedolyn sydd â chyfrifoldeb rhiant arfer hawliau diogelu data'r plentyn ar ei ran. Os byddwch yn dibynnu ar gydsyniad rhiant fel eich sail gyfreithlon dros brosesu, bydd yn arfer da darparu dau hysbysiadau preifatrwydd ar wahân, un a anelir at y plentyn yn ogystal ag un at yr oedolyn cyfrifol.

Os gwelwch yn dda, darllenwch ganllawiau Swyddfa'r Comisiynydd Gwybodaeth ar yr hawl i gael gwybod: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

15.2 Hawl mynediad – a elwir hefyd yn 'gais gwrthrych am wybodaeth'

O dan y GDPR, mae hawl gan unigolion i ofyn am gopi o'r holl wybodaeth a ddelir amdanynt gennych chi (h.y. eu data personol). Gall yr wybodaeth hon fod ynghadw ar gyfrifiadur a/neu mewn cofnodion papur penodol.

Nid yw'r GDPR yn pennu sut y dylid gwneud cais dilys. Felly, gall unigolyn gyflwyno cais mynediad gwrthrych i chi ar lafar neu mewn ysgrifen. Cyn darparu copïau o'r wybodaeth, rhaid i chi gael sicrwydd mai'r gwrthrych ei hunan sy'n gofyn am yr wybodaeth, a bod hawl ganddo i'w chael. Gellwch ofyn i'r ceisydd am ragor o wybodaeth; mae hawl gennych, er enghraifft, i ofyn am dystiolaeth adnabod sy'n cynnwys ffotograff neu brawf cyfeiriad.

Os digwydd i chi gael cais mynediad gwrthrych, bydd rhaid i chi ddarparu copi o'r wybodaeth **yn ddi-dâl**. Fodd bynnag, cewch godi 'ffi resymol' pan fo cais yn ddi-sail neu'n rhy feichus, yn enwedig os gwneir ceisiadau droeon, neu os gofynnir am gopïau o'r un wybodaeth. Dylech geisio ymateb i gais cyn gynted ag y bo modd, ond ddim hwyrach nag un mis ar ôl cael y cais

Mae nifer o esemptiadau rhag y gofyniad i ddarparu gwybodaeth yn ymateb i gais mynediad gwrthrych. Rhai enghreifftiau fyddai: braint broffesiynol gyfreithiol; negodiadau gyda gwrthrych y data, os byddai ymateb i'r cais yn debygol o beryglu'r negodiadau hynny; rhagamcanion a chynlluniau rheolwyr, pe bai datgelu gwybodaeth yn niweidiol i gynnal y busnes; a geirdaon cyfrinachol. Mae'n bwysig deall na cheir defnyddio'r esemptiadau hyn fel y safiad diofyn, a bod rhaid cyfiawnhau pob defnydd unigol o esemptiad.

Yn benodol, dylech gofio y **gallech** fod yn esempt rhag darparu data sy'n gysylltiedig â gwneud rhaglenni (gan gynnwys deunydd crai *(rushes)*) o dan yr esemptiad arbennig ar gyfer dibenion newyddiadurol, academaidd, llenyddol neu artistig a bennir ym mharagraff 26 o Ran 5 o Atodlen 2 i'r DDD 2018.

Os penderfynwch beidio â darparu copi o'i ddata i'r unigolyn, dylech esbonio eich penderfyniad a hysbysu'r unigolyn bod hawl ganddo i wneud cwyn i Swyddfa'r Comisiynydd Gwybodaeth ac i geisio gorfodi ei hawliau trwy rwymedi barnwrol.

Os gwelwch yn dda, darllenwch y canllawiau ar hawl mynediad ar wefan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Mae canllawiau pellach ar yr esemptiadau a sut i'w defnyddio ar gael gan y Comisiynydd Gwybodaeth. Mae cod ymarfer newydd ar drin ceisiadau mynediad gwrthrych ar gael hefyd ar wefan y Comisiynydd:

http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

Nodyn i Gynhyrchwyr:
Pan fo'r cais yn ymwneud â deunydd rhaglen gan gynnwys deunydd crai *(rushes)*, dylech ymgynghori â'r darlledwr sy'n eich comisiynu er mwyn trafod unrhyw seiliau cyfreithiol a golygyddol dilys a allai gyfiawnhau gwrthwynebu, neu a oes angen cymryd unrhyw gamau pellach cyn datgelu (h.y. dileu rhag tramgwyddo yn erbyn hawliau rhywun arall).

15.3 Yr hawl i gywiriad

Mae'r GDPR yn cynnwys yr hawl i unigolion gael cywiro data personol sy'n anghywir, neu gwblhau'r data os ydynt yn anghyflawn. Caiff unigolyn wneud cais am gywiriad ar lafar neu mewn ysgrifen.

Cewch wrthod cydymffurfio â chais am gywiriad os yw'r cais yn amlwg yn ddi-sail neu'n rhy feichus neu o natur ailadroddus. Cewch ofyn am "ffi resymol" am ymdrin â'r cais. Os nad ydych yn sicr pwy yw'r person sy'n gwneud y cais, gellwch ofyn am ragor o wybodaeth.

Os bodlonir chi fod yr wybodaeth sydd gennych eisoes yn ddilys, dylech roi gwybod i'r unigolyn fod y data personol yn eich barn chi yn gywir, ac na fyddwch yn diwygio'r data.

Os byddwch yn cywiro neu'n cwblhau'r data, a chithau eisoes wedi datgelu'r data personol i eraill, rhaid i chi gysylltu â phob un o'r derbynwyr i'w hysbysu o'r cywiriad neu'r cwblhad – oni fydd hynny'n amhosibl neu'n afresymol o feichus. Os gofynnir i chi, rhaid i chi hefyd roi gwybod i'r unigolyn pwy oedd y derbynwyr.

Bydd gennych **un mis calendr** i ymateb i gais. Dylech esbonio eich penderfyniad a rhoi gwybod i'r unigolyn fod hawl ganddo i wneud cwyn i Swyddfa'r Comisiynydd Gwybodaeth ac i geisio gorfodi ei hawliau trwy rwymedi barnwrol.

Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar yr hawl i gywiriad yma:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Nodyn i Gynhyrchwyr:
Pan fo'r cais yn ymwneud â deunydd rhaglen, cyn gwneud unrhyw ddatgeliad ynglŷn â chywiriad, hwyrach y byddwch yn dymuno ymgynghori â'r darlledwr sy'n eich comisiynu, oherwydd gall fod seiliau cyfreithiol a golygyddol dilys dros wrthwynebu unrhyw newidiadau yn yr wybodaeth.

15.4 Yr hawl i ddileu, yr hawl i fynd yn angof

Mae'r GDPR yn cyflwyno hawl i unigolion ddileu data personol. Cyfeirir hefyd at yr hawl hon i ddileu fel yr 'hawl i fynd yn angof'. Caiff unigolyn wneud cais am ddilead naill ai ar lafar neu mewn ysgrifen. Nid yw hon yn hawl absoliwt, ac mewn amgylchiadau penodol yn unig y mae'n bodoli. Bydd gennych **un mis** i ymateb i gais. Os nad fyddwch yn sicr pwy yw'r person sy'n gwneud y cais, cewch ofyn iddo am ragor o wybodaeth.

Bydd gan unigolion yr hawl i gael dileu eu data personol:

- pan nad oes angen y data personol bellach at y diben y'u casglwyd yn wreiddiol neu pan ydych yn dibynnu ar gydsyniad fel eich sail gyfreithlon dros gadw'r data, a'r unigolyn tynnu ei gydsyniad yn ôl;
- pan ydych yn dibynnu ar fuddiannau dilys, neu pan fo'r unigolyn yn gwrthwynebu prosesu ei ddata, ac nid oedd buddiant dilys gor-redol ar gyfer parhau'r prosesu hwn;
- os buoch yn prosesu'r data yn anghyfreithlon (gan dorri'r egwyddor diogelu data gyntaf);
- pan ydych yn prosesu'r data personol at ddibenion marchnata uniongyrchol, a'r unigolyn yn gwrthwynebu;
- pan wneir hynny i gydymffurfio â rhwymedigaeth gyfreithiol; neu os oeddech wedi prosesu'r data personol i gynnig 'gwasanaethau cymdeithas wybodaeth' i blentyn.
- **Gwybodaeth plant**: Rhoddir pwyslais ar yr hawl i gael dileu data personol pan fo'r cais yn ymwneud â data a gasglwyd gan blant. Os byddwch yn prosesu data a gasglwyd gan blant, dylech roi pwys ychwanegol ar gais am ddilead os prosesir y data ar sail cydsyniad a roddwyd gan blentyn - yn enwedig unrhyw brosesu o'r data personol ar y Rhyngrwyd. Bydd hyn yn parhau'n wir pan fydd gwrthrych y data bellach wedi peidio â bod yn blentyn, oherwydd y posibilrwydd nad oedd, fel plentyn, yn llwyr ymwybodol o'r risgiau a oedd yn gysylltiedig â'r prosesu ar yr adeg y cydsyniodd.

Pa bryd nad oes hawl i gael dileu/i fynd yn angof?

Nid yw'r hawl hon yn bodoli os yw'r prosesu yn angenrheidiol am un o'r rhesymau canlynol:

- i arfer yr hawl i ryddid mynegiant a gwybodaeth;
- i gydymffurfio â rhwymedigaeth gyfreithiol;
- i gyflawni tasg a wneir er budd y cyhoedd neu wrth arfer awdurdod swyddogol;
- at ddibenion archifo er budd y cyhoedd, ymchwil wyddonol, ymchwil hanesyddol, neu ddibenion ystadegol, os byddai dileu yn gwneud cyflawni prosesau o'r fath yn amhosibl neu'n amharu arnynt yn ddifrifol;
- ar gyfer sefydlu, gweithredu neu amddiffyn hawliadau cyfreithiol.

Os gwelwch yn dda, darllenwch ganllawiau Swyddfa'r Comisiynydd Gwybodaeth ar yr hawl i gael dileu:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

15.5 Yr hawl i gyfyngu

Mae gan unigolion hawl i gyfyngu neu atal prosesu eu data personol. Nid yw hon yn hawl absoliwt, ac mewn amgylchiadau penodol yn unig y mae'n bodoli. Pan gyfyngir ar brosesu, bydd hawl gennych chi i storio'r data personol, ond nid i'w defnyddio. Caiff unigolyn wneud cais am gyfyngu naill ai ar lafar neu mewn ysgrifen. Bydd gennych **un mis calendr** i ymateb i unrhyw gais.

Mae'r GDPR yn awgrymu nifer o wahanol ddulliau y gellid eu defnyddio i gyfyngu data, gan gynnwys:

- symud y data i system brosesu arall dros dro;
- peri na fydd y data ar gael i ddefnyddwyr; neu
- dynnu data a gyhoeddir oddi ar wefan dros dro.

Cewch wrthod cydymffurfio â chais am gyfyngu os yw'r cais yn amlwg yn ddi-sail neu'n rhy feichus, gan ystyried hefyd a yw'r cais yn ailadroddus.

Gellir darllen canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar yr hawl i gyfyngu prosesu yn:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

15.6 Yr hawl i gludadwyedd data

Mae'r hawl i gludadwyedd data yn caniatáu i unigolion gyrchu ac ailddefnyddio'u data personol at eu dibenion eu hunain ar draws gwahanol wasanaethau. Mae'n caniatáu iddynt symud, copïo neu drosglwyddo data personol yn hwylus a diogel o un amgylchedd TG i amgylchedd arall heb amharu ar ddefnyddiadwyedd y data. Rhaid i chi ymateb rhag blaen i gais ynglŷn â chludadwyedd data, yn ddi-oed ac o fewn **un mis calendr** fan bellaf ar ôl cael y cais.

Nid yw'r hawl i gludadwyedd data yn bodoli ac eithrio:

- yn achos data personol a ddarparwyd gan unigolyn i reolydd data;
- pan fo'r prosesu yn seiliedig ar gydsyniad yr unigolyn neu ar gyfer cyflawni contract; a
- phan gyflawnir y prosesu hefyd yn awtomataidd.

Cewch wrthod cydymffurfio â chais am gludadwyedd data os yw'r cais yn amlwg yn ddi-sail neu'n rhy feichus, gan ystyried hefyd a yw'r cais yn ailadroddus.

Gellir darllen canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar gludadwyedd data yn:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

15.7 Yr hawl i wrthwynebu

Mae'r GDPR yn rhoi i unigolion yr hawl i wrthwynebu prosesu eu data personol mewn rhai amgylchiadau. Caiff unigolyn fynegi ei wrthwynebiad ar lafar neu mewn ysgrifen. Bydd gennych **un mis calendr** i ymateb i wrthwynebiad. Mae gan unigolion hawl i wrthod i'w data gael eu prosesu os yw'r data'n cael eu trin naill ai: ar sail buddiannau dilys; ar gyfer cyflawni tasg sydd er budd y cyhoedd/arfer awdurdod swyddogol (gan gynnwys proffilio); ar gyfer marchnata uniongyrchol (gan gynnwys proffilio); neu ar gyfer prosesu at ddibenion ymchwil wyddonol/hanesyddol neu ystadegau.

Os byddwch yn prosesu data ar gyfer cyflawni tasg gyfreithiol neu at ddiben dilys eich sefydliad chi neu farchnata uniongyrchol, rhaid i chi hysbysu'r unigolion o'u hawl i wrthwynebu "ar yr adeg y cyfathrebir gyntaf" a hefyd yn eich hysbysiad preifatrwydd. Os bydd yr unigolyn yn gwrthwynebu, rhaid iddo wneud hynny ar "sail sy'n ymwneud â'i sefyllfa benodol ef neu hi".

Os byddwch yn prosesu data at ddibenion ymchwil, rhaid i unigolyn fod â "sail sy'n ymwneud â'i sefyllfa benodol ef neu hi" er mwyn arfer ei hawl i wrthwynebu. Yn yr ymchwil a gyflawnir gennych, os bydd prosesu data personol yn angenrheidiol ar gyfer cyflawni tasg sydd er budd y cyhoedd, ni fydd yn ofynnol eich bod yn cydymffurfio ag unrhyw wrthwynebiad i'r prosesu.

Ni fydd angen i chi atal prosesu – os gellwch ddangos bod sail ddilys a grymus dros brosesu, sy'n drech na buddiannau, hawliau a rhyddid yr unigolyn; neu fod y prosesu ar gyfer sefydlu, gweithredu neu amddiffyn hawliadau cyfreithiol.

Gwybodaeth plant: mae gan blant yr un hawl ag oedolion i wrthwynebu prosesu eu data personol ar gyfer marchnata uniongyrchol, ac felly rhaid i chi roi'r gorau i wneud hynny os yw plentyn (neu rywun sy'n gweithredu ar ei ran) yn gofyn i chi beidio; mae plant yn teilyngu camau diogelu penodol pan ddefnyddir eu data personol at ddibenion marchnata.

Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar yr hawl i wrthwynebu yn:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

15.8 Hawliau mewn perthynas â gwneud penderfyniadau yn awtomataidd, gan gynnwys proffilio

Mae'r GDPR yn berthnasol i bob penderfyniad awtomataidd a wneir ynghylch unigolyn. Mae'r hawliau hyn yn berthnasol pan fo'r penderfyniad yn cael effaith gyfreithiol neu effaith sylweddol gyffelyb arall ar yr unigolion y prosesir eu data. Mae hyn yn gyfyngedig i benderfyniadau cyfan gwbl awtomataidd, a wneir heb unrhyw ymyrraeth ddynol, ac i broffilio (sef prosesu data personol yn awtomataidd er mwyn gwerthuso nodweddion penodol unigolion).

Yn ei hanfod, mae Erthygl 22 o'r GDPR yn gwahardd gwneud y math hwn o benderfyniad oni fodlonir un o'r amodau isod. Felly, ni chewch wneud penderfyniadau yn y modd hwn ac eithrio pan fo penderfyniad:

- yn angenrheidiol ar gyfer ymuno mewn neu gyflawni contract; neu
- wedi ei awdurdodi gan gyfraith yr Undeb Ewropeaidd neu pa bynnag gyfraith aelod-wladwriaeth y mae'r rheolydd yn ddarostyngedig iddi; neu
- yn seiliedig ar gydsyniad penodol yr unigolyn.

Rhaid i chi ganfod a oes unrhyw ran o'r prosesu yn dod o fewn cwmpas y ddarpariaeth hon; ac os oes, gwneud yn sicr eich bod:

- yn rhoi gwybodaeth i'r unigolion ynghylch y prosesu;
- yn trefnu ffyrdd hwylus iddynt ofyn am ymyrraeth ddynol neu herio penderfyniad;
- cyflawni gwiriadau rheolaidd i gael sicrwydd fod eich systemau yn gweithio fel y bwriadwyd

Gwybodaeth plant: Ni ddylech wneud penderfyniadau ynghylch plentyn ar sail prosesu awtomataidd yn unig, (gan gynnwys proffilio), os yw'r penderfyniadau'n cael effaith gyfreithiol neu effaith sylweddol gyffelyb ar y plentyn. Os byddwch yn proffilio plant, rhaid i chi roi gwybodaeth eglur iddynt am yr hyn y byddwch yn ei wneud gyda'u data personol. Ni ddylech fanteisio'n annheg ar unrhyw ddiffyg dealltwriaeth neu hyglwyfedd.

Yn gyffredinol, dylech osgoi proffilio plant at ddibenion marchnata. Rhaid i chi barchu hawl absoliwt y plentyn i wrthwynebu proffilio sy'n gysylltiedig â marchnata uniongyrchol, a rhoi'r gorau i wneud hynny os bydd y plentyn yn gofyn i chi. Mae'n bosibl i hysbysebu ymddygiadol gael 'effaith sylweddol gyffelyb' ar blentyn. Mae hynny'n dibynnu ar natur y dewisiadau a'r ymddygiad y ceisir dylanwadu arno.

Ceir rhagor o wybodaeth am weithredu hyn mewn cysylltiad â phlant ar wefan Swyddfa'r Comisiynydd Gwybodaeth:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar hawliau mewn perthynas â gwneud penderfyniadau awtomataidd yn:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

16. Esemptiadau

16.1 Newyddiadurol, academaidd, artistig a llenyddol

Mae'r esemptiad hwn yn seiliedig ar Erthygl 85(2) o'r GDPR am resymau sy'n ymwneud â rhyddid mynegiant a gwybodaeth, a gellir ei weld ym mharagraff 26 o Ran 5 o Atodlen 2 i'r DDD 2018. O ran sylwedd, mae ymddangos mai'r un yw criteria'r esemptiad hwn a'r esemptiad blaenorol yn y DDD 1998. O dan Erthygl 85(2) o'r GDPR mae'n ofynnol gwrthbwyso hawliau sylfaenol sydd yn Siarter Hawliau Sylfaenol yr Undeb Ewropeaidd. Erthygl 11 o'r Siarter yw rhyddid mynegiant a gwybodaeth, tra bo Erthyglau 7 ac 8 yn darparu ar gyfer hawliau i breifatrwydd a diogelu data.

Mae'n bwysig nodi nad oes esemptiad llwyr yn y DDD 2018 rhag diogelu data ac ni ddylid defnyddio'r esemptiad fel pe bai'n hollgynhwysfawr (neu'n agos at hynny). Hyd yn oed pan fo'r esemptiad ar gael, rhag darpariaethau penodol yn unig y mae'n esemptio, a hynny yn unig i'r graddau y mae'r darpariaethau hynny yn anghydnaws â'r diben arbennig.

16.1.1 **Diben arbennig**: O dan y DDD 2018, ystyr 'dibenion arbennig' yw'r dibenion newyddiadurol, academaidd (mae 'academaidd' yn ddarpariaeth newydd), artistig a llenyddol. Mae'r dibenion arbennig hyn wedi'u hesemptio rhag rhai amodau penodol o dan y GDPR, ar yr amod y bodlonir y canlynol:

- y prosesir y data sydd dan sylw gyda'r bwriad o gyhoeddi deunydd newyddiadurol, academaidd, artistig a/neu lenyddol,
- rhaid i'r rheolydd data fod yn *credu yn rhesymol*, ar ôl rhoi ystyriaeth benodol i bwysigrwydd arbennig y buddiant cyhoeddus mewn rhyddid mynegiant, y byddai cyhoeddi er lles y cyhoedd, a
- rhaid i'r rheolydd data fod yn *credu yn rhesymol* y byddai gweithredu'r ddarpariaeth a restrir yn y GDPR yn anghydnaws â'r diben newyddiadurol, academaidd, artistig a/neu lenyddol.
- Os rhagdybio bod y criteria hyn wedi'u bodloni, bydd rheolydd data yn esempt rhag cydymffurfio â'r hawliau a'r rhwymedigaethau yn y GDPR mewn perthynas â phrosesu data personol, er enghraifft wrth wneud rhaglen. Rhestrir manylion yr hyn a esemptir ym mharagraff 26(9) o Atodlen 2 i'r DDD 2018. Yn dilyn yr egwyddor atebolrwydd o fewn y GDPR, mae'n bwysig ei fod yn bosib ichi ddogfennu a chofnodi eich penderfyniad ar weithrediad yr esempliad.

16.1.2 **Mesurau diogelwch**: Mae'n bwysig nodi nad oes esemptiad o dan y DDD 2018[1] mewn perthynas â'r egwyddor bod rhaid prosesu data personol gan weithredu mesurau technegol a threfniadol priodol i sicrhau y'u prosesir yn deg chyfreithlon.[2]

16.1.3 **Codau ymarfer**: Ychwanegir at bwysigrwydd y codau ymarfer pan fo cyhoeddwr yn bwriadu dibynnu ar yr esemptiad. Mae'r DDD 2018[3] yn darparu'n benodol fod *rhaid* i reolydd data, wrth ffurfio'i gred y byddai cyhoeddi er budd y cyhoedd, yn rhoi sylw priodol i'r codau ymarfer perthnasol, sef Canllawiau Golygyddol y BBC, Cod Darlledu Ofcom a Chod ymarfer y Golygyddion. Caiff yr Ysgrifennydd Gwladol ychwanegu codau ymarfer eraill hefyd.[4]

16.1.4 **Ataliad statudol:** Mae adran 176 yn cadw mewn bodolaeth y mecanwaith "ataliad" sy'n rhwystro defnyddio diogelu data i gael gwaharddeb cyn-cyhoeddi (mewn perthynas â deunydd nas cyhoeddwyd, neu a gyhoeddwyd am lai na 24 awr). Fodd bynnag, mae adran 174(3)(b) o'r DDD 2018 yn darparu y caiff Swyddfa'r Comisiynydd Gwybodaeth wneud penderfyniad i'r perwyl naill ai nad yw'r data personol yn cael eu prosesu at y dibenion arbennig yn unig, neu nad yw'r data yn cael eu prosesu gyda'r bwriad o gyhoeddi deunydd newyddiadurol nas cyhoeddwyd eisoes.

16.1.5 **Troseddau data**: Cyflwynwyd troseddau newydd ochr yn ochr ag amddiffyniadau penodol ar sail newyddiaduraeth sydd er budd y cyhoedd, yn adrannau 170-171 o'r DDD 2018. Bellach, yn ychwanegol at y drosedd bresennol o gaffael ar ddata personol yn anghyfreithlon, mae hefyd yn drosedd i alluogi i unigolyn gael ei adnabod o'r newydd o ddata personol oedd gynt wedi ei gofnodi yn ddienw. Oherwydd y risg o ardaro ar newyddiaduraeth ymchwiliol, darperir amddiffyniadau penodol sy'n adleisio'r esemptiad dibenion arbennig, ar gyfer pob un o'r troseddau.

16.1.6 **Canllawiau a rhwymedigaethau adolygu ac adrodd:** Mae cyfrifoldebau Swyddfa'r Comisiynydd Gwybodaeth, fel y corff gwarchod sy'n goruchwylio'r cyfryngau, wedi eu cynyddu fel a ganlyn:

- Mewn perthynas â diwydiant y cyfryngau, disgwylir i Swyddfa'r Comisiynydd Gwybodaeth baratoi canllawiau ar y modd y gall unigolyn geisio iawn gan gorff yn y cyfryngau os tybia nad yw'r corff hwnnw wedi cydymffurfio â'r ddeddfwriaeth diogelu data. Ni fydd hyn yn berthnasol, o anghenraid, i lwyfannau ar-lein [5]

[1] mewn perthynas â'r rhwymedigaeth o dan Erthygl 5(f) o'r GDPR
[2] gweler adran 32(2)(a) o Ddeddf Diogelu Data 1998 a pharagraff 26(9)(i) o Ran 5 o Atodlen 2 i Ddeddf Diogelu Data 2018)
[3] Deddf Diogelu Data 2018, Atodlen 2, Rhan 5, paragraff 26(5)
[4] Deddf Diogelu Data 2018, Atodlen 2, Rhan 5, paragraff 26(7)
[5] Deddf Diogelu Data 2018, adran 179

- Mae gofyn i Swyddfa'r Comisiynydd Gwybodaeth ymgynghori, paratoi a chyflwyno cod ymarfer i'r Ysgrifennydd Gwladol ar gyfer ei gymeradwyo gan y Senedd yn cynnwys canllawiau ymarferol ar brosesu data personol mewn modd cydymffurfiol at ddibenion newyddiaduraeth ac ar arferion da dymunol sy'n rhoi sylw i fuddiannau gwrthrychau'r data ac ar bwysigrwydd arbennig budd y cyhoedd mewn cysylltiad â rhyddid mynegiant a gwybodaeth.
- Bydd Swyddfa'r Comisiynydd Gwybodaeth yn cynnal adolygiadau rheolaidd o'r modd y mae'r cyfryngau'n cydymffurfio â'r ddeddfwriaeth diogelu data, ac yn adrodd am ei chanfyddiadau wrth yr Ysgrifennydd Gwladol.[6]
- Rhaid i'r Ysgrifennydd Gwladol yntau, ar wahân, adrodd wrth y Senedd am y defnydd a wneir o weithdrefnau datrys anghydfod y cyfryngau a'u heffeithiolrwydd, mewn achosion sy'n cynnwys honiadau o dorri'r ddeddfwriaeth diogelu data; ac yn benodol, adrodd am unrhyw weithdrefnau datrys anghydfod a ddarperir gan y rhai sy'n gorfodi'r codau ymarfer ar gyfer cyrff perthnasol yn y cyfryngau.[7] Bydd hyn yn cynnwys Sefydliad Annibynnol Safonau'r Wasg (IPSO), y cwmni monitro annibynnol IMPRESS, ac o bosibl hefyd Ofcom (hwyrach yn anfwriadol, oherwydd nad oes diffiniad o'r hyn a olygir wrth 'weithdrefn datrys anghydfod amgen') i'r graddau y mae cod Ofcom yn berthnasol i gyhoeddwyr ar-alw.

Mae Swyddfa'r Comisiynydd Gwybodaeth yn diweddaru ei chanllawiau ar gyfer diwydiant y cyfryngau. Yn y cyfamser, dylech siarad â'r darlledwr sy'n eich comisiynu, neu ymgynghori â chyfreithiwr ynglŷn â'r esemptiadau yn y DDD 2018, Atodlen 2, Rhan 5, paragraff 26.

17. Atebolrwydd a llywodraethu

Mae atebolrwydd yn ofyniad newydd o dan y GDPR – rydych yn gyfrifol am gydymffurfio â'r GDPR, a rhaid i chi **hefyd**, bellach, allu dangos eich bod yn cydymffurfio. Bydd sefydlu polisïau perthnasol yn fodd i arddangos eich dull o fynd ati i gydymffurfio.

Mae angen i chi gymryd camau technegol a threfniadol priodol i fodloni'r gofynion atebolrwydd. Dylai fod yn hawdd i sefydliadau, sydd eisoes wedi ymateb i ofynion cydymffurfiaeth y DDD 1998 trwy fabwysiadu agwedd 'arferion gorau', ymaddasu i'r gofynion newydd. Fodd bynnag, dylech adolygu eich arferion ar gyfer y GDPR.

Ystyrir bod y materion canlynol yn berthnasol o ran arddangos atebolrwydd

- Mabwysiadu a gweithredu polisïau diogelu data;
- Dogfennu eich gweithgareddau prosesu; cofnodi ac adrodd am doriadau data personol;
- Creu, gweithredu a gwella mesurau diogelwch priodol;
- Sefydlu contractau ysgrifenedig gyda chyrff sy'n prosesu data personol ar eich rhan;
- Mabwysiadu dull o 'ddiogelu data o'r cychwyn ac fel anghenraid' trwy gynnal asesiadau o'r effaith ar breifatrwydd a 'phreifatrwydd o'r dechrau', gan gynnwys mesurau fel lleihau i'r eithaf y nifer o ddata a gesglir, defnyddio technegau ffugenwi a gwella'r nodweddion diogelwch;
- Defnyddio **asesiadau effaith diogelu data (AEDDau)** ar gyfer dulliau o ddefnyddio data personol sy'n debygol o achosi risg uchel i fuddiannau unigolion;
- Cydymffurfio â'r **codau ymddygiad/cynlluniau ardystio** a gymeradwyir;
- Penodi swyddog diogelu data (pan fo'n angenrheidiol); a
- Sicrhau bod lefel dealltwriaeth ac ymwybyddiaeth o ddiogelu data yn uchel ymhlith eich staff;

17.1 Asesiadau effaith diogelu data (AEDDau) *[Data Protection Impact Assessments DPIA]*

Mae asesiadau effaith diogelu data (AEDDau) bellach yn ofyniad cyfreithiol pan fo'r prosesu yn debygol o achosi risg uchel i fuddiannau unigolion. Er mwyn asesu lefel y risg, rhaid i chi ystyried y tebygolrwydd yn ogystal ag enbydrwydd unrhyw effaith ar unigolion. Proses yw AEDD i'ch helpu i adnabod a lleihau'r risgiau diogelu data sy'n deillio o brosiect. Os tybiwch fod AEDD yn angenrheidiol, dylech drafod gyda'r darlledwr sy'n eich comisiynu a gofyn am fewnbwn ganddo.

Mae Swyddfa'r Comisiynydd Gwybodaeth wedi cyhoeddi rhestr o enghreifftiau o'r mathau o weithrediadau prosesu y byddai AEDD yn ofynnol ar eu cyfer o dan y GDPR. Bwriad y rhestr yw helpu rheolwyr data i ddeall pa bryd y bydd AEDD yn ofynnol yn awtomatig, a pha bryd yr ystyrid y byddai'n arfer da.

[6] Deddf Diogelu Data 2018, adran 178 ac Atodlen 17
[7] Deddf Diogelu Data 2018, adran 179

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Nodir y pethau a ddylai fod yn rhan o unrhyw AEDD yn: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Mae Swyddfa'r Comisiynydd Gwybodaeth hefyd wedi darparu awgrym o dempled ar gyfer AEDD: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

17.2 Diogelu data o'r cychwyn ac fel anghenraid

O dan y GDPR, mae rhwymedigaeth gyffredinol arnoch i weithredu mesurau technegol a threfniadol i ddangos eich bod wedi gwneud diogelu data yn rhan annatod o'ch gweithgareddau prosesu.

Mae Swyddfa'r Comisiynydd Gwybodaeth yn gweithio i ddiweddaru'r canllawiau hyn er mwyn adlewyrchu darpariaethau'r GDPR. Yn y cyfamser bydd y canllawiau cyfredol yn fan cychwyn da i'r sefydliadau. Gweler gwefan Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

17.3 Sicrhau bod data yn ddienw

Nid yw'r GDPR yn berthnasol i wybodaeth ddienw. Mae sicrhau bod data yn ddienw yn broses lle tynnir ymaith unrhyw ddynodwyr personol, uniongyrchol ac anuniongyrchol, a allai beri i unigolyn gael ei adnabod. Gellir defnyddio dull effeithiol o sicrhau bod data yn ddienw er mwyn cyhoeddi data a fyddai, fel arall, yn ddata personol

Mae Swyddfa'r Comisiynydd Gwybodaeth yn diffinio'r broses o sicrhau bod data yn ddienw fel y broses o roi data mewn ffurf nad yw'n caniatáu i unigolion gael eu hadnabod, ac nad yw adnabyddiaeth o'r fath yn debygol o ddigwydd trwy gyfuno'r data gyda data eraill. Unwaith y bydd data yn gwbl ddienw, ni fydd y data wedyn o fewn cwmpas y GDPR a byddant yn haws eu defnyddio.

Er mwyn canfod a ellir sicrhau bod data yn ddienw, a hynny mewn modd effeithiol, mae'n synhwyrol cynnal asesiad trwyadl o'r risg y gallai unrhyw sefydliad neu aelod o'r cyhoedd adnabod unrhyw unigolyn oddi wrth y data a ryddheir – naill ai ar eu pen eu hunain neu o'u cyfuno â gwybodaeth arall.

Dyfais ddefnyddiol ar gyfer hyn yw'r **Prawf Ymyrrwr Ewyllysgar *[Motivated Intruder Test]*** sy'n golygu ystyried a fyddai modd i "ymyrrwr" adfer adnabyddiaeth o'r unigolyn *pe* bai ganddo'r ewyllys i geisio gwneud hynny. Rhagdybir bod yr 'ymyrrwr ewyllysgar' yn berson sy'n cychwyn heb unrhyw wybodaeth flaenorol, ond sy'n awyddus i adnabod yr unigolyn a oedd yn berchen ar y data personol y tarddodd y data dienw ohonynt. Gellir cymryd bod yr ymyrrwr ewyllysgar yn rhesymol fedrus, ond nad oes ganddo unrhyw wybodaeth arbenigol.

Gall trefniant trydydd parti dibynadwy (TTD) fod yn arbennig o effeithiol pan fo nifer o sefydliadau yn dymuno cydweithio ar brosiect a newid y data personol y maent yn ei ddal i fod yn ddata dienw. Yn arferol, bydd y TTD yn gweithredu fel storfa ddata lle gall y gwahanol sefydliadau sy'n cymryd rhan yn y prosiect ddatgelu eu data personol.

Gellid defnyddio'r dechneg o drawsnewid data personol yn ddata dienw er mwyn galluogi aelodau o gynulleidfa i rannu eu straeon a'u profiadau pan fo'r data sydd ar gael yn sensitif. Er enghraifft, pe byddai unigolion yn dymuno cyfrannu at stori am eu profiadau gyda'r GIG, hwyrach y byddai angen cydgrynhoi'r cyfraniadau hynny neu sicrhau eu bod yn ddienw, a hynny er mwyn ategu at y stori heb ei chysylltu ag unigolyn penodol. Gellid hefyd ddefnyddio dulliau i sicrhau bod data yn ddienw pan fo sefydliad yn dymuno rhannu data at ddibenion ymchwil.

Gweler Swyddfa'r Comisiynydd Gwybodaeth:
http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

18. Diogelwch data personol ('Egwyddor Diogelwch')

Un o egwyddorion allweddol y GDPR yw y dylech brosesu data personol trwy ddefnyddio 'mesurau technegol a threfniadol priodol'. Mae'r egwyddor hon yn disodli ac yn adlewyrchu'r gofyniad blaenorol o dan y DDD 1998, sef 'bod â mesurau technegol a threfniadol priodol'.

Ystyr hyn yw fod angen i chi sicrhau diogelwch priodol, rhag i'r data personol a ddelir gennych gael eu colli neu'u difrodi, yn ddamweiniol neu'n fwriadol. Mae'r egwyddor diogelwch yn ymestyn y tu hwnt storio a thrawsyrru'r data. Yn yr egwyddor, cwmpesir nid yn unig seiberddiogelwch, ond pob agwedd arall hefyd ar y modd y byddwch yn prosesu data personol.

Mae'r hyn sy'n 'briodol' ar eich cyfer chi yn dibynnu ar amgylchiadau eich cwmni. Dylech adolygu'r data personol a ddelir gennych a'r ffordd y byddwch yn eu defnyddio, er mwyn asesu pa mor werthfawr, sensitif neu gyfrinachol ydynt – yn ogystal â pha niwed neu drallod a achosid pe difrodid y data. Byddai Swyddfa'r Comisiynydd Gwybodaeth, wrth ystyried unrhyw ddirwy weinyddol, yn edrych ar ba fesurau technegol a threfniadol yr ydych wedi eu sefydlu.

O dan y DDD 1998, cyhoeddodd Swyddfa'r Comisiynydd Gwybodaeth nifer o eitemau canllaw ar wahanol agweddau ar ddiogelwch TG. Bydd Swyddfa'r Comisiynydd Gwybodaeth yn diweddaru ei chanllawiau maes o law, i adlewyrchu gofynion yr GDPR.

19. Arferion a argymhellir ar gyfer diogelwch data personol

Dylai cwmni cynhyrchu adolygu'n rheolaidd y modd y mae'n storio'i holl ddata personol, gan gynnwys data'r unigolion hynny y cesglir eu data personol wrth wneud y rhaglen, er mwyn asesu a ellir gwella'r mesurau diogelwch a sefydlwyd. Yn ogystal, dylid cyfyngu nifer y rhai a awdurdodir i gael mynediad i'r data, ac i'w haddasu, eu datgelu neu'u dileu.

Os caiff data personol eu colli, eu newid neu'u dinistrio yn ddamweiniol, dylai fod yn bosibl i chi eu hadfer, a thrwy hynny osgoi unrhyw niwed neu drallod i'r unigolion.

Po leiaf o ddata personol a gedwir gennych, isaf fydd lefel eich risg. Felly, trwy baratoi rhestrau cadwraeth a'u defnyddio byddwch yn lleihau'r risg o golli data. Fodd bynnag, bydd angen bob amser i chi gadw rhai data personol, a dylech eu cadw mewn diogelwch priodol. Rhoddir rhai awgrymiadau sut i wneud hynny isod.

19.1 Diogelwch ar y safle

- A ellir cadw ffeiliau cynhyrchu a ffeiliau eraill mewn cypyrddau cloëdig, a/neu oes yna storfa ddiogel, ar y safle neu oddi arno?

- A yw'r mesurau diogelwch gwybodaeth ar y cyfrifiaduron swyddfa a'r rhwydweithiau yn ddigonol? A yw gwybodaeth o'r cyfrineiriau yn gyfyngedig, ac a fyddwch yn diweddaru'r cyfrineiriau yn rheolaidd?

- A fyddwch yn cyfyngu mynediad i ffeiliau cyfrifiadurol i'r rhai sydd arnynt angen mynediad mewn gwirionedd? A fyddwch yn allgofnodi o'r cyfrifiaduron dros nos, neu'n eu cadw o dan glo pan nad oes neb o gwmpas?

- A ddiogelir eich systemau cyfrifiadurol gan waliau tân a mesurau gwrthfeirysol digonol? A roddir canllawiau i'r staff ar y gofal sy'n angenrheidiol wrth agor negeseuon e-bost ac atodiadau, neu ymweld â gwefannau anghyfarwydd?

- A yw'r trefniadau ar gyfer copïau wrth gefn o'r data personol yn ddigonol, rhag eu dinistrio'n ddamweiniol?

- A yw sgriniau cyfrifiadur, hysbysfyrddau a byrddau gwyn wedi'u lleoli'n ddigon pell oddi wrth ffenestri, neu o olwg y cyhoedd, rhag datgelu data personol yn ddamweiniol? A gymerir camau priodol i sicrhau na all ymwelwyr diawdurdod weld unrhyw ddogfennau papur?

- A ydych yn rheoli mynediad i'r adeilad ac yn gweithredu mesurau diogelwch digonol a rhesymol? A fydd ymwelwyr yn cael eu goruchwylio neu'u monitro yn ddigonol yng nghyffiniau gwybodaeth bersonol neu wybodaeth gyfrinachol arall?

Os ydych yn gweithredu system deledu cylch cyfyng (CCTV), a yw'r system yn cydymffurfio â'r cod ymarfer CCTV a ddarperir gan Swyddfa'r Comisiynydd Gwybodaeth? – Sylwch nad yw'r canllawiau canlynol gan Swyddfa'r Comisiynydd Gwybodaeth eto wedi'u diweddaru i gydymffurfio â'r GDPR – ond byddent yn fan cychwyn da: http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

I gael arweiniad pellach r ddiogelwch TG ar gyfer y GDPR, cyfeirier at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

19.2 Diogelwch oddi ar y safle

- A ydych yn caniatáu mynd â chyfrifiaduron, gliniaduron, disgiau cyfrifiadurol, cofion bach ac ati o'r safle? Os ydych, a weithredir diogelwch cyfrineiriau priodol ar gyfer data personol, data categori arbennig, data troseddol, data plant, data ariannol (neu ddata eraill megis manylion cyswllt prif dalentau)? A ddefnyddir amgryptio lefel-uchel yn y ffolderi perthnasol, neu yn y cyfrifiaduron, disgiau cyfan, neu a drefnir math arall o ddiogelwch effeithiol? Pe bai rhywun yn dwyn y cyfarpar, a fyddai'r data personol wedi'u diogelu?

- A ydych wedi ystyried canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar weithredu amgryptio: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/implementing-encryption/ A yw'r cynhyrchion amgryptio a ddefnyddir wedi'u hardystio i fodloni safonau cyfredol y GDPR?

- A ydych wedi gweithredu'n briodol ar y cyngor a roddir yng nghanllawiau Swyddfa'r Comisiynydd Gwybodaeth, i'r perwyl y dylid amgryptio pob dyfais gludadwy sy'n cynnwys data personol safon FIPS 140-2 (modiwlau cryptograffig, meddalwedd a chaledwedd) neu FIPS – 197 (neu fel y cynghorir fel arall o bryd i'w gilydd gan Swyddfa'r Comisiynydd Gwybodaeth)? Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth yn: http://ico.org.uk/news/current_topics/Our_approach_to_encryption Sylwch nad yw'r canllawiau hyn eto wedi'u diweddaru trwy gynnwys gwybodaeth ychwanegol am y GDPR.

- A yw cyfrineiriau eich dyfeisiau gwaith symudol wedi eu cloi a/neu'u codio?

- Wrth ddefnyddio band eang pan fo dolen ar gael, a oes dulliau diogelu priodol wedi eu sefydlu ar gyfer mynediad i'r wybodaeth, h.y. diogelwch cyfrinair/ rhwydwaith diogel?

- A roddir canllawiau addas ar ddiogelu, dychwelyd a/neu ddinistrio dogfennau, cofion bach, a/neu DVDs y bydd angen eu symud o'r safle? A oes mecanweithiau gennych sy'n sicrhau bod y staff yn gwybod am y canllawiau hyn ac yn eu dilyn? A ydych wedi dosbarthu'r Canllawiau Diogelwch Data i Griwiau Cynhyrchu? A fyddwch yn darparu cyfleoedd i'r staff ennill dealltwriaeth o'r rhwymedigaethau o dan y GDPR? A yw'r staff/criw yn gwybod â phwy i gysylltu os digwydd toriad data?

- A oes system wedi ei sefydlu i olrhain data a gludir oddi ar y safle ac a ddychwelir?

- A wneir darpariaethau digonol i storio papurach cynhyrchu, dalennau galwadau a ffurflenni rhyddhau pan fônt oddi ar y safle, rhag i'r dogfennau hyn gael eu gadael yma ac acw?

- A fydd unrhyw ddata personol, data categori arbennig neu ddata plant yn cael eu cadw mewn system storio sy'n seiliedig ar gwmwl neu offeryn cydweithio? Os felly, a oes mesurau diogelwch digonol wedi eu sefydlu i sicrhau diogelwch y data sy'n defnyddio'r system storio honno?

- Os ydych yn defnyddio unrhyw wasanaethau neu gyflenwyr ar-lein (er enghraifft, Mailchimp i ddosbarthu cylchlythyrau neu Dropbox i anfon ffeiliau), eich cyfrifoldeb chi yw sicrhau eu bod yn cydymffurfio a'r GDPR. Gellwch ganfod a ydynt yn cydymffurfio trwy ymweld â'u gwefan i ddarllen eu polisi preifatrwydd a'u telerau defnyddio, neu wirio bod eu telerau'n cynnwys geiriad proseswyr priodol, neu gellwch anfon e-bost atynt i ofyn. Os nad yw'r gwasanaethau a chyflenwyr yn cydymffurfio â'r GDPR, hwyrach y dylech chwilio am wasanaethau amgen sydd yn cydymffurfio, gan mai eich cwmni chi a fydd yn atebol yn y pen draw.

19.3 Casglu a gwaredu gwybodaeth

- A fyddwch yn copïo a dosbarthu cofnodion papur ac electronig yn ddiangen? A yw'r staff yn ymwybodol y dylid bod yn ofalus i beidio gadael copïau o ddogfennau ger y llungopïwr, sganiwr neu beiriant ffacs?

- A oes peiriannau rhwygo a/neu finiau neu flychau ailgylchu "diogel" ar gael yn hwylus i waredu dogfennau a phapurau a allai gynnwys data personol, ac a fyddir yn atgoffa'r staff i'w defnyddio yn briodol?

- A gymerir y gofal angenrheidiol wrth ffacsio data personol, i sicrhau mai'r derbynnydd a fwriedir yn unig a fydd yn cael yr wybodaeth, a hynny ar yr adeg y'i hanfonir? Mae Swyddfa'r Comisiynydd Gwybodaeth yn argymell y dylid lleihau nifer y ffacsys a anfonir, gan fod ffacsio wedi bod yn achos nifer o gosbau ariannol sifil. Pan fo anfon ffacs yn anochel, argymhellir y dylid anfon cadarnhad o dderbyniad unrhyw ddata personol a anfonir mewn ffacs.

- A yw cyflogeion a gweithwyr yn deall y gall datgelu data personol, hyd yn oed ar lafar, fod yn doriad o'r GDPR ac a ydynt yn gwybod pa bryd y mae'n briodol datgelu?

- Os byddwch yn cael cais am wybodaeth gan yr heddlu, ni fydd gorfodaeth arnoch i ddatgelu'r wybodaeth. Fodd bynnag, gellwch ddewis darparu'r wybodaeth os bodlonir uwch-aelod o'ch cwmni eich bod wedi cydymffurfio â'r canllawiau canlynol (nid yw'r rhain eto wedi'u diweddaru yn unol â'r GDPR):

  http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/SECTION_29_GPN_V1.ashx.

  Pan fo cais am wybodaeth yn ymwneud â deunydd rhaglen neu deunydd crai *(rushes)*, dylech ymgynghori â'r darlledwr sy'n eich comisiynu cyn gwneud unrhyw ddatgeliad, oherwydd gall fod seiliau cyfreithiol a golygyddol dilys dros wrthwynebu datgelu.

- Pan ddaw gwaith cynhyrchu i ben, dylai uwch-aelodau o'r staff adolygu pa gofnodion o ddata personol y gellir yn gyfreithlon eu cadw neu'u dinistrio.

- Os ydych yn gwerthu neu'n gwaredu cyfrifiaduron, disgiau neu gofion bach, a ydych wedi cymryd camau priodol i sicrhau bod unrhyw ddata personol a storiwyd ar y dyfeisiau hynny wedi'u dileu yn ddiogel, neu eu symud o gyrraedd defnyddwyr newydd y dyfeisiau?

- Dylid ystyried a oes rheswm dilys dros gadw cofnodion. Er enghraifft, dylid dinistrio cofnodion ceiswyr sioe cwis nad ydynt yn ymddangos yn y rhaglen derfynol, oni fyddant wedi rhoi'u caniatâd i gadw'r cofnodion ar gyfer cyfres neu sioeau eraill yn y dyfodol, neu pan fo rheswm busnes neu gyfreithiol dilys arall dros eu cadw (er enghraifft, os cafodd ceisydd ddamwain yn y gwrandawiad, a bod angen cadw ei gofnodion am resymau iechyd a diogelwch); ond hwyrach y bydd angen cadw cofnodion actor na chafodd ei gynnwys yn y toriad terfynol, o leiaf am gyfnod cyfyngedig ar gyfer gwrandawiadau, er enghraifft.

- Pan ddaw cyflogaeth aelodau o'ch staff i ben, a fyddant yn cael eu hatgoffa neu'u gorfodi, i **adael ar ôl a/neu ddileu** pob data cyfrinachol a/neu ddata personol priodol?

20. A gaf i ddefnyddio'r data personol ar gyfer ein prosiectau eraill neu ar gyfer marchnata ?

Rhaid i chi ddefnyddio data personol, yn unig, at y dibenion cyfyngedig hynny y casglwyd y data ar eu cyfer neu y rhoddwyd y data i chi. Er enghraifft, mae'n bosibl y darparwyd y data personol gan gyfrannwr ar gyfer rhaglen benodol yn unig, ac nid ar gyfer unrhyw ddiben arall. Mae hynny'n golygu na chewch werthu, dosbarthu na darparu'r data personol hynny mewn unrhyw ffurf arall i unrhyw drydydd parti, ac eithrio pan fo hynny'n angenrheidiol ar gyfer cynhyrchu'r Rhaglen ac elwa arni.

Fodd bynnag, os yw'r person ei hunan yn cydsynio'n benodol i chi gysylltu ag ef drachefn yn y dyfodol, i ymdrin â rhaglenni eraill neu i gael gwybodaeth farchnata, neu gysylltu â chyflogeion ynghylch cyfleoedd gwaith ac ati, yna caniateir i chi wneud hynny (dylid adolygu cydsyniadau o'r fath yn rheolaidd). Os byddwch yn dymuno darparu negeseuon marchnata electronig i unigolion (er enghraifft, SMS neu e-byst marchnata), bydd eu cydsyniad penodol yn ofynnol (ac eithrio mewn amgylchiadau cyfyngedig). Gellir cytuno hynny, er enghraifft, pan fo cyfrannwr yn llofnodi'r ffurflen, neu wrth ymuno mewn contract gyda chyflogai neu weithiwr rhaid gwneud yn eglur ar ba sail gyfreithlon y byddwch yn defnyddio'r data.

21. Defnyddio offer olrhain ar lein, megis briwsion.

21.1 Briwsion

Mae Rheoliadau Preifatrwydd a Chyfathrebu Electronig (Cyfarwyddeb CE) 2003 *[Privacy and Electronic Communications (EC Directicve) Regulations 2003 (PECR)]* yn ymdrin â defnyddio briwsion a gwybodaeth arall y gellir eu storio ar ddyfais unigolyn. Darn bach o ddata yw briwsionyn, sydd yn aml yn cynnwys dynodydd adnabod unigryw, a anfonir o gyfrifiadur

gwefan i borwr eich cyfrifiadur neu ffôn symudol chi (y cyfeirir atynt yma fel "eich dyfais") ac a storir wedyn ar ddisg caled eich dyfais. Rhaid i unrhyw gwmni sy'n defnyddio briwsion neu dechnoleg gyffelyb gymryd y camau angenrheidiol i gydymffurfio â'r Rheoliadau.

Rhaid peidio â defnyddio briwsion neu ystrywiau cyffelyb oni fydd y tanysgrifiwr neu ddefnyddiwr y cyfarpar terfynol perthnasol:

- yn cael gwybodaeth eglur a chynhwysfawr am y dibenion o storio'r wybodaeth ac o sicrhau mynediad iddi; ac
- wedi rhoi ei gydsyniad.

Rhoddir cyngor ar ddefnyddio briwsion ar wefan Swyddfa'r Comisiynydd Gwybodaeth yn y canllawiau "*Guidance on the use of cookies and similar technologies*":
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies

Bydd Rheoliadau Preifatrwydd a Chyfathrebu Electronig (Cyfarwyddeb CE) 2003 yn cael eu diweddaru yn ystod 2019. Y bwriad yw rhoi gwybodaeth mwy eglur i unigolion, a gwell rheolaeth iddynt ar y modd y defnyddir briwsion pan ymwelir â gwefannau a gwasanaethau. Yn ogystal, bwriedir rhwystro'r 'naid-flychau'' sy'n ymddangos ar y sgrîn ar chwap, ac yn pledu'r defnyddwyr gyda cheisiadau am gael glanio briwsion. Clywir rhagor am y datblygiadau newydd hyn.

21.2 Data lleoliad

Mewn rhai amgylchiadau, gall y sefydliadau sy'n cynnig gwasanaethau mewn cysylltiad â ffonau clyfar a'r System Leoli Fyd-eang GPS fod yn prosesu data lleoliad (er enghraifft, codau post, cyfeirnodau map, neu unrhyw ddata eraill sy'n datgelu lleoliad daearyddol dyfais symudol y defnyddiwr). Mae'r Rheoliadau Preifatrwydd a Chyfathrebu Electronig yn pennu rheolau tra manwl ynglŷn â chasglu a defnyddio data lleoliad, ac yn gwneud 'cydsyniad' yn ofynnol ar gyfer casglu data am leoliad defnyddwyr dyfeisiadau symudol. Rhaid i gyhoeddwyr beidio â chasglu gwybodaeth am leoliad daearyddol eu defnyddwyr oni cheisir, a hyd nes ceisir, y cydsyniad hwnnw.

Gellid defnyddio data lleoliad mewn nifer o wahanol ffyrdd; er enghraifft, gan gwmnïau sy'n cynhyrchu cynnwys digidol megis apiau, neu ar gyfer personoleiddio, er enghraifft mewn apiau tywydd i roi gwybodaeth fanwl am y tywydd yn lleol, neu mewn 'cynnwys a gynhyrchir gan ddefnyddwyr', er enghraifft pan wahoddir aelodau o gynulleidfa i dynnu ffotograffau, tagio eu lleoliad, a lanlwytho'r ffotograffau i wefan y rhaglen.

Os gwelwch yn dda, darllenwch ganllawiau Swyddfa'r Comisiynydd Gwybodaeth ar ddata lleoliad:
https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/

22. A oes arnaf angen Swyddog Diogelu Data?

Mae'r GDPR yn cyflwyno rhwymedigaeth i benodi Swyddog Diogelu Data os yw eich gweithgareddau craidd yn galw am fonitro unigolion yn systematig a rheolaidd ar raddfa fawr (er enghraifft, olrhain ymddygiad ar-lein); neu brosesu data categorïau arbennig neu ddata sy'n ymwneud â throseddau a chollfarnau ar raddfa fawr.

Gellwch benodi Swyddog Diogelu Data os dymunwch, hyd yn oed pan nad yw hynny'n ofynnol. Os penderfynwch benodi Swyddog Diogelu Data yn wirfoddol, dylech wybod y bydd yr un gofynion a thasgau yn perthyn i'r swydd â phe bai penodi Swyddog Diogelu Data wedi bod yn orfodol. Rhaid i chi, beth bynnag, pa un a yw'r GDPR yn eich gorfodi i benodi Swyddog Diogelu Data ai peidio, sicrhau bod gan eich sefydliad staff ac adnoddau digonol i gyflawni eich rhwymedigaethau o dan y GDPR. Os penderfynwch nad oes angen i chi benodi Swyddog Diogelu Data, yn wirfoddol nac oherwydd bodloni'r criteria uchod, byddai'n ddoeth cofnodi'r penderfyniad hwnnw er mwyn arddangos eich cydymffurfiaeth â'r egwyddor atebolrwydd. Os na fyddwch yn penodi Swyddog Diogelu Data statudol, mae'n bwysig peidio â galw'r person cyfrifol yn 'Swyddog Diogelu Data' pan nad honno yw ei rôl mewn gwirionedd; byddai 'Rheolwr Data' yn deitl mwy priodol.

- Os byddwch yn penodi Swyddog Diogelu Data, y person hwnnw fydd y pwynt cyswllt cyntaf ar gyfer Swyddfa'r Comisiynydd Gwybodaeth ac ar gyfer yr unigolion y byddwch yn prosesu eu data. Bydd angen i chi gyhoeddi manylion eich Swyddog Diogelu Data, a darparu copi ohonynt i Swyddfa'r Comisiynydd Gwybodaeth.

- Rhaid i'r Swyddog Diogelu Data fod yn annibynnol, yn arbenigwr ar ddiogelu data, a chael adnoddau digonol; a rhaid iddo adrodd wrth reolwyr ar y lefel uchaf. Gall yr Swyddog Diogelu Data fod yn un o gyflogeion presennol y sefydliad

neu'n berson a benodir o'r tu allan (ar yr amod nad yw ei rôl yn gwrthdaro nac yn creu gwrthdrawiad). Mewn rhai achosion, gall nifer o sefydliadau benodi un Swyddog Diogelu Data rhyngddynt.

- Dylai'r Swyddog Diogelu Data fonitro cydymffurfiaeth â'r GDPR, eich polisïau diogelu data a'ch gweithgareddau diogelu data mewnol; codi'r ymwybyddiaeth o faterion diogelu data; hyfforddi staff; cynnal archwiliadau mewnol; a monitro a chynghori ynghylch asesiadau effaith diogelu data;

- Bydd rhaid i chi ddarparu adnoddau digonol (sef amser digonol, adnodd ariannol a seilwaith, yn ogystal â staff pan fo'n briodol) i alluogi'r Swyddog Diogelu Data i gyflawni ei rwymedigaethau GDPR a chynnal lefel ei wybodaeth arbenigol

Gellir gweld canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar Swyddogion Diogelu Data yn: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

23. Beth os daw toriad neu golled diogelwch neu ddatgeliad diawdurdod i'ch sylw?

Ystyr toriad data personol yw toriad diogelwch sy'n arwain at ddinistrio data personol yn ddamweiniol neu'n anghyfreithlon, eu colli, eu newid, neu eu datgelu neu achosi mynediad atynt yn ddiawdurdod. Mae hyn yn cynnwys toriadau o ganlyniad i achosion damweiniol a bwriadol, a newid data heb ganiatâd. Gall toriad, felly, gynnwys mwy na cholli data personol yn unig.

Os daw toriad o'r GDPR i'ch sylw, dylech roi gwybod ar unwaith i'ch rheolwr llinell, i'r Swyddog Diogelu Data neu i'r uwch-aelod o'ch staff sy'n gyfrifol am faterion GDPR, gan fod angen gweithredu yn ddi-oed.

Dylech hefyd weithredu ar unwaith i ganfod pa niwed y gellid ei achosi i'r person(au) perthnasol.

Os yw'r toriad yn ymwneud â deunydd rhaglen (er enghraifft, yn ymwneud â chyfranwyr, cystadleuwyr neu dalent) dylech roi gwybod cyn gynted ag y bo modd hefyd i'r darlledwr sy'n eich comisiynu, a chymryd pa bynnag gamau eraill a allai fod yn fuddiol.

23.1 Pa doriadau y dylem hysbysu'r Swyddfa'r Comisiynydd Gwybodaeth yn eu cylch?

O dan y GDPR, pan fo toriad data personol wedi digwydd, rhaid i'r rheolydd hysbysu'r awdurdod goruchwyliol (sef Swyddfa'r Comisiynydd Gwybodaeth yn achos y Deyrnas Unedig) **heblaw fod y** toriad yn annhebygol o achosi risg i hawliau a rhyddid unigolion. Felly, bydd angen i chi asesu pa mor debygol a pha mor enbyd yw'r risg i hawliau a rhyddid pobl o ganlyniad i'r toriad. Os yw'n debygol y bydd y risg yn uchel, bydd yn rhaid hysbysu Swyddfa'r Comisiynydd Gwybodaeth; os yw'n annhebygol y bydd risg uchel i hawliau neu ryddid person, ni fydd rhaid i chi hysbysu Swyddfa'r Comisiynydd Gwybodaeth o'r toriad. Fodd bynnag, os penderfynwch nad oes angen adrodd am y toriad, bydd angen i chi allu cyfiawnhau'r penderfyniad hwnnw. Felly, bydd rhaid dogfennu'r toriad yn ogystal â'ch penderfyniad chi ynghylch adrodd amdano. Bydd angen i chi asesu hyn ar sail pob achos unigol, gan ystyried yr holl ffactorau perthnasol. Mae'n bosibl hefyd y bydd angen i chi hysbysu gwrthrychau'r data perthnasol, os yw'r risg i hawliau a rhyddid unigolion yn uchel, a hwythau o ganlyniad yn debygol o ddioddef niwed.

Os yw'r toriad yn ymwneud â deunydd rhaglen dylech roi gwybod cyn gynted ag y bo modd hefyd i'r darlledwr sy'n eich comisiynu, a chymryd pa bynnag gamau eraill a allai fod yn fuddiol. Gall fod yn briodol weithiau i chi benderfynu, ar y cyd â'ch comisiynwr, mai'r darlledwr yw'r sefydliad gorau i hysbysu Swyddfa'r Comisiynydd Gwybodaeth, os y darlledwr yw'r rheolydd data. Dylai prosesydd hysbysu rheolydd data yn ddi-oed os daw toriad data i'w sylw.

Os yw'r toriad yn un y mae angen adrodd amdano, rhaid i chi hysbysu Swyddfa'r Comisiynydd Gwybodaeth (os yw'r risg yn uchel) o fewn 72 awr fan hwyraf ar ôl dod yn ymwybodol o'r toriad. Os cymerwch yn hwy na hyn, rhaid i chi roi rhesymau addas dros yr oedi. Yn achos toriad sy'n effeithio ar unigolion mewn gwahanol wledydd yn yr Undeb Ewropeaidd, mae'n bosibl nad Swyddfa'r Comisiynydd Gwybodaeth fydd yr awdurdod goruchwyliol arweiniol.

Mae Swyddfa'r Comisiynydd Gwybodaeth yn darparu canllawiau ychwanegol ar adrodd wrth Swyddfa'r Comisiynydd Gwybodaeth: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

23.2 Beth yw'r cosbau am ddatgelu heb awdurdod?

Mae Swyddfa'r Comisiynydd Gwybodaeth yn ymchwilio i bob toriad o'r GDPR. Gall Swyddfa'r Comisiynydd Gwybodaeth osod sancsiynau (gan gynnwys sancsiynau troseddol) ar gwmnïau a geir yn euog o doriad. Mae pŵer gan Swyddfa'r Comisiynydd Gwybodaeth i osod dirwyon ar sefydliadau o hyd at €10m neu 2 y cant o gyfanswm trosiant y sefydliad, ynghyd â sancsiynau eraill, am doriad o'r GDPR megis peidio ag adrodd am doriad wrth y rheoleiddiwr o fewn 72 awr. Am doriad difrifol megis toriad diogelwch sy'n arwain at niwed sylweddol i unigolion, gellir gosod dirwy arnoch o hyd at €20m neu 4 y cant o gyfanswm eich trosiant.

24. Difrodi enw da

Yn ychwanegol at y sancsiynau statudol y caiff Swyddfa'r Comisiynydd Gwybodaeth eu gosod ar gwmni, pan fo toriad yn digwydd achosir risg sylweddol i enw da'r cwmni neu'r darlledwr. Gall y sefyllfa waethygu pan fo'r toriad yn ymwneud â thalent. Mae modd i feirniadaeth yn y wasg, a anelir at gwmni cynhyrchu, talent neu ddarlledwr achosi difrod sylweddol. Ar ben hynny, bydd cyfranwyr yn llai parod i ddatgelu data personol i gwmni cynhyrchu os credant na fydd y cwmni'n cadw eu data'n ddiogel.

25. Canllawiau a gwybodaeth bellach

Mae canllawiau a gwybodaeth bellach gan Swyddfa'r Comisiynydd Gwybodaeth ar gael yn www.ico.org.uk.

- I gael rhagor o wybodaeth am DDD 2018, gellir ymweld â: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- Y GDPR:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

DIWEDD