

Polisi diogelu data (sy'n cydymffurfio gyda'r GDPR)

1. Cyflwyniad

Mae'r polisi diogelu data hwn yn nodi sut mae Mentrau Iaith Cymru ("ni", "ni") yn trin data personol ein cwsmeriaid, cleientiaid, cyflenwyr, cyflogai, gweithwyr, gwirfoddolwyr a thrydydd bartïon eraill.

Mae'r polisi diogelu data hwn yn berthnasol i'r holl ddata personol yr ydym yn ei brosesu waeth beth fo'r cyfryngau y caiff y data hwnnw ei storio arno os yw'n ymwneud â chyflogai, gweithwyr, cwsmeriaid, cleientiaid, ymddireidolwyr, cyflenwyr, cyfranddalwyr, defnyddwyr y wefan neu unrhyw ddeiliad arall o ddata.

Mae'r polisi diogelu data hwn yn berthnasol i holl bersonél y cwmni ("chi"). Rhaid i chi ddarllen, deall a chydymffurfio â'r polisi diogelu data hwn wrth brosesu data personol ar ein rhan. Mae'r polisi diogelu data hwn yn nodi'r hyn yr ydym yn ei ddisgwyl gennych er mwyn inni gydymffurfio â'r gyfraith berthnasol. Mae eich cydymffurfiaeth â'r polisi diogelu data hwn yn orfodol. Gall unrhyw anghydfurfiaeth gyda'r polisi diogelu data hwn arwain at gamau disgyblu.

Mae'r polisi diogelu data hwn yn ddogfen fewnol ac ni ellir ei rannu gyda thrydydd parti, cleientiaid na rheoleiddwyr heb ganiatâd blaenorol gan ein Swyddog Diogelu Data ("DPO").

2. Cwmpas

Mae'r DPO yn gyfrifol am oruchwylio'r polisi diogelu data hwn.

Cysylltwch â'r DPO gydag unrhyw gwestiynau ynghylch gweithrediad y polisi diogelu data hwn neu'r Rheoliad Gwarchod Data Cyffredinol (y "GDPR") neu os oes gennych unrhyw bryderon nad yw'r polisi diogelu data hwn yn cael ei ddilyn. Yn benodol, rhaid i chi gysylltu bob amser â'r DPO yn yr amgylchiadau canlynol:

(a) os nad ydych yn siŵr o'r sail gyfreithlon yr ydych yn dibynnu arni i brosesu data personol (gan gynnwys y buddiannau cyfreithlon a ddefnyddiwyd gennym ni);

(b) os oes angen i chi ddibynnu ar ganiatâd a / neu angen i chi gasglu caniatâd penodol;

(c) os ydych chi'n ansicr ynghylch y cyfnod cadw ar gyfer prosesu'r data personol;

(ch) os ydych chi'n ansicr ynghylch pa fesurau diogelwch y mae angen i chi eu gweithredu i ddiogelu data personol;

(d) os bu torri rheolau data personol;

(dd) os ydych chi'n ansicr ar ba sail i drosglwyddo data personol y tu allan i'r Ardal Economaidd Ewropeaidd (AEE);

(e) os oes arnoch angen unrhyw gymorth i ddelio ag unrhyw hawliau sy'n cael eu hawlio gan ddeiliad data;

(f) pryd bynnag y byddwch yn cymryd rhan mewn gweithgaredd prosesu newydd, neu weithgaredd sydd wedi newid yn sylweddol, ac mae'n debygol o fod angen Asesiad Effaith Preifatrwydd Data (DPIA) neu gynllun i ddefnyddio data personol at ddibenion heblaw am yr hyn a gasglwyd;

(ff) Os ydych chi'n bwriadu ymgymryd ag unrhyw weithgareddau sy'n ymwneud â phrosesu awtomatig, gan gynnwys proffilio neu wneud penderfyniadau awtomatig;

(g) Os oes angen help arnoch i gydymffurfio â'r gyfraith berthnasol wrth gynnal gweithgareddau marchnata uniongyrchol; neu

(ng) os oes angen help arnoch gydag unrhyw gontractau neu feysydd eraill mewn perthynas â rhannu data personol gyda thrydydd partion.

3. Egwyddorion diogelu data personol

Rydym yn cadw at yr egwyddorion sy'n ymwneud â phrosesu data personol a nodir yn y GDPR sy'n gofyn am ddata personol:

(a) Wedi'i brosesu yn gyfreithlon, yn deg ac mewn modd tryloyw.

(b) Wedi'i gasglu yn unig at ddibenion penodol, eglur a dilys.

(c) Digonol, perthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y caiff ei brosesu ar ei gyfer.

(ch) Cywir a, lle bo angen, yn cael ei ddiweddarau.

(d) Heb ei gadw mewn ffurf sy'n caniatáu adnabod deiliaid data yn hwy nag sy'n angenrheidiol at y dibenion y prosesir y data.

(f) Wedi'i brosesu mewn modd sy'n sicrhau ei ddiogelwch gan ddefnyddio mesurau technegol a threfniadol priodol i ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon ac yn erbyn colli, dinistrio neu ddifrod damweiniol.

(g) Heb ei drosglwyddo i wlad arall heb fod mesurau diogelwch priodol yn eu lle.

(h) Wedi'i ddarparu ar gyfer deiliaid data a bod gan y deiliaid data hawl i ymarfer rhai hawliau mewn perthynas â'u data personol.

Rydym yn gyfrifol am, a rhaid i ni allu dangos cydymffurfiaeth â'r egwyddorion diogelu data a restrir uchod.

4. Cyfreithlondeb, tegwch, tryloywder

4.1 Cyfreithlondeb a thegwch

Rhaid prosesu data personol yn gyfreithlon, yn deg ac yn dryloyw mewn perthynas â'r deiliad data.

Dim ond yn rhesymol ac yn gyfreithlon y gallwch chi gasglu, prosesu a rhannu data personol ac at ddibenion penodol. Mae'r GDPR yn cyfyngu ein gweithredoedd o ran data personol at ddibenion cyfreithlon penodol. Ni fwriedir i'r cyfyngiadau hyn atal prosesu, ond sicrhau ein bod yn prosesu data personol yn deg a heb effeithio'n andwyol ar ddeiliad y data.

Mae'r GDPR yn caniatáu prosesu at ddibenion penodol, ac mae rhai ohonynt wedi'u nodi isod:

- (a) bod y deiliad data wedi rhoi ei ganiatâd;
- (b) bod y prosesu yn angenrheidiol ar gyfer perfformio contract gyda'r deiliad data;
- (c) i fodloni ein rhwymedigaethau cydymffurfio cyfreithiol;
- (ch) i ddiogelu buddiannau hanfodol y deiliad data; neu
- (e) i ddilyn ein buddiannau cyfreithlon at ddibenion lle na chant eu gwahardd oherwydd bod y prosesu yn rhagfarnu buddiannau neu hawliau sylfaenol a rhyddid deiliaid data. Mae angen nodi'r dibenion y byddwn yn prosesu data personol ar gyfer buddiannau cyfreithlon yn y rhybuddion preifatrwydd perthnasol.

4.2 Caniatâd

Mae deiliad data yn caniatáu i ni brosesu eu data personol os ydynt yn dangos cytundeb yn glir naill ai trwy ddatganiad neu gamau cadarnhaol i'r prosesu. Mae caniatâd yn gofyn am gamau cadarnhaol fel bod aros yn dawel, blychau wedi ticio eisioes neu anactifedd yn annhebygol o fod yn ddigonol. Os rhoddir caniatâd mewn dogfen sy'n ymdrin â materion eraill, yna rhaid cadw'r caniatâd ar wahân i'r materion eraill hynny.

Rhaid i ddeiliaid data allu tynnu'n ôl eu caniatâd i'r prosesu yn hawdd ac ar unrhyw adeg, a rhaid anrhydeddu y dymuniad yn brydlon. Efallai y bydd angen

adnewyddu caniatâd os ydych chi'n bwriadu prosesu data personol ar gyfer diben gwahanol ac anghydnaws i'r hyn a gafodd ei ddatgelu pan oedd y deiliad data wedi rhoi ei ganiatad yn y lle cyntaf.

Oni bai y gallwn ddibynnu ar sail gyfreithiol arall o brosesu, fel arfer mae angen caniatâd penodol ar gyfer prosesu data personol sensitif, ar gyfer gwneud penderfyniadau awtomatig ac ar gyfer trosglwyddiadau data trawsffiniol. Fel rheol, byddwn yn dibynnu ar sail gyfreithiol arall (lle nad oes angen caniatâd penodol) i brosesu'r rhan fwyaf o fathau o ddata sensitif. Os oes angen caniatâd penodol, mae'n rhaid i chi roi rhybudd prosesu teg i'r deiliad data i gasglu, caniatâd penodol.

4.3 Tryloywder (hysbysu deiliaid data)

Mae'r GDPR yn ei gwneud yn ofynnol i reolwyr data ddarparu gwybodaeth fanwl, benodol i ddeiliaid data yn dibynnu ar p'run ai casglwyd y wybodaeth yn uniongyrchol o ddeiliaid data neu o rywle arall. Rhaid darparu gwybodaeth o'r fath trwy rhybuddion preifatrwydd priodol ac mae'n rhaid eu bod yn gryno, yn dryloyw, yn ddealladwy, yn hawdd eu cael, ac mewn iaith glir a phriodol fel y gall deiliad data eu deall yn hawdd.

Pryd bynnag y byddwn yn casglu data personol yn uniongyrchol o ddeiliaid data, gan gynnwys ar gyfer adnoddau dynol neu ddibenion cyflogaeth, mae'n rhaid i ni ddarparu'r holl wybodaeth sy'n ofynnol gan y GDPR i ddeiliad y data, gan gynnwys hunaniaeth y rheolwr data a'r DPO, sut a pham y byddwn yn defnyddio'r data, y broses, os byddwn yn datgelu, diogelu a chadw'r data personol hwnnw trwy rybudd prosesu teg. Mae'n ofynnol i gyflwyno'r rhybudd prosesu teg pan fydd y deiliad data yn darparu'r data personol yn gyntaf.

Pan gesglir data personol yn anuniongyrchol (er enghraifft, gan drydydd parti neu ffynhonnell sydd ar gael i'r cyhoedd), rhaid i chi ddarparu'r holl wybodaeth sy'n ofynnol gan y GDPR i'r deiliad data cyn gynted ag y bo modd ar ôl casglu / derbyn y data. Rhaid ichi hefyd wirio bod y data personol yn cael ei gasglu gan y trydydd parti yn unol â'r GDPR ac ar sail sy'n adlewyrchu ein prosesu arfaethedig o'r data personol hwnnw.

5. Cyfyngiad pwrpas

Rhaid casglu data personol yn unig at ddibenion penodol, eglur a dilys. Ni ddylid ei brosesu ymhellach mewn unrhyw fodd sy'n anghydnaws â'r dibenion hynny.

Ni allwch ddefnyddio data personol ar gyfer dibenion newydd, gwahanol neu anghydnaws o'r hyn a ddatgelwyd pan gafodd ei gael gyntaf oni bai eich bod wedi rhoi gwybod i'r deiliad data y dibenion newydd hynny ac maent wedi cydsynio iddynt lle bo angen.

6. Lleihau data

Rhaid i ddata personol fod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y caiff ei brosesu ar ei gyfer.

Gallwch ond prosesu data personol os yw'n rhan o ddyletswyddau eich swydd i wneud hynny. Ni allwch brosesu data personol am unrhyw reswm nad yw'n gysylltiedig â'ch swydd.

Dim ond ar gyfer eich swydd y gallwch chi gasglu data personol: peidiwch â chasglu data gormodol a pheidiwch â gwneud copïau diangen. Sicrhewch fod unrhyw ddata personol a gasglwyd yn ddigonol ac yn berthnasol i'r dibenion a fwriadwyd.

Rhaid ichi sicrhau, pan nad oes angen data personol mwyach at ddibenion penodol, caiff ei ddileu, ei ddinistrio'n ddiogel neu ei wneud yn anhysbys yn unol â'n canllawiau cadw data.

7. Cywirdeb

Rhaid i ddata personol fod yn gywir a, lle bo angen, cael ei diweddarau. Rhaid ei gywiro neu ei ddileu yn ddi-oed pan fydd yn anghywir.

Byddwch yn sicrhau bod y data personol yr ydym yn ei ddefnyddio a'i gadw yn gywir, yn gyflawn, wedi'i ddiweddarau ac yn berthnasol i'r diben y cafodd ei gasglu. Rhaid i chi wirio cywirdeb unrhyw ddata personol yn y man casglu ac yn rheolaidd ar ôl hynny. Rhaid i chi gymryd pob cam rhesymol i ddinistrio neu ddiwygio data personol anghywir neu anghyfredol.

8. Cyfyngiad storio

Ni ddylid cadw data personol mewn ffurf adnabyddadwy am gyfnod hwy nag sy'n angenrheidiol ar gyfer y dibenion y prosesir y data.

Rhaid i chi beidio â chadw data personol mewn ffurf sy'n caniatáu adnabod deiliad y data am fwy nag y mae ei angen ar gyfer dibenion neu ddibenion busnes cyfreithlon yr oeddem yn ei gasglu yn wreiddiol, gan gynnwys at ddibenion bodloni unrhyw ofynion cyfreithiol, cyfrifyddu neu adrodd.

Byddwn yn cynnal polisiau a gweithdrefnau cadw i sicrhau bod data personol yn cael ei ddileu ar ôl amser rhesymol at y dibenion y'i cynhelir, oni bai bod cyfraith yn mynnu bod data o'r fath yn cael ei chadw am isafswm cyfnod.

Byddwch yn cymryd pob cam rhesymol i ddinistrio neu ddileu holl ddata personol o'n systemau nad sydd yn ofynnol mwyach yn unol â'n holl bolisiau perthnasol.

Mae hyn yn cynnwys gofyn i drydydd partïon ddileu data o'r fath lle bo'n berthnasol.

9. Cywirdeb diogelwch a chyfrinachedd

9.1 Diogelu Data Personol

Rhaid sicrhau data personol trwy fesurau technegol a threfniadol priodol yn erbyn prosesu anawdurdodedig neu anghyfreithlon, ac yn erbyn colli, dinistrio neu ddifrod damweiniol.

Byddwn yn datblygu, gweithredu a chynnal mesurau diogelu sy'n briodol i'n maint, ein cwmpas a'n busnes, yr adnoddau sydd ar gael i ni, y swm o ddata personol yr ydym yn berchen arno neu yn ei gynnal ar ran eraill a risgiau a nodwyd (gan gynnwys defnyddio amgryptio a ffugenwi lle bo hynny'n berthnasol).

Byddwn yn gwerthuso a phrofi effeithiolrwydd y mesurau diogelu hynny yn rheolaidd er mwyn sicrhau diogelwch ein prosesu data personol.

Rydych chi'n gyfrifol am ddiogelu'r data personol sydd gennym. Rhaid i chi weithredu mesurau diogelwch rhesymol a phriodol rhag prosesu data personol anghyfreithlon neu heb awdurdod, ac yn erbyn colled damweiniol neu ddifrod o ddata personol. Rhaid i chi ymarfer gofal penodol wrth ddiogelu data personol sensitif rhag colled, mynediad, defnydd neu ddatgeliad heb ganiatâd. Yn benodol mae hyn yn cynnwys:

(a) gwaharddiad ar arbed data personol i gyfrifiaduron personol neu ddyfeisiau eraill;

(b) ceisio caniatâd gan y DPO cyn i unrhyw ddata personol gael ei dynnu oddi ar ein safle;

(c) defnyddio cyfrineiriau cryf;

(ch) cloi sgriniau cyfrifiadur;

(d) sicrhau bod dogfennau sy'n cynnwys data personol a data personol sensitif yn cael eu cadw'n ddiogel;

(dd) amgryptio data wrth ei drosglwyddo'n electronig i bartïon eraill; ac

(e) ystyried defnyddio allweddi / codau ar wahân i ddi-enwi data fel na ellir adnabod deiliad y data.

Rhaid i chi ddilyn yr holl weithdrefnau a thechnolegau a roddwn ar waith i gynnal diogelwch pob data personol o'r pwynt casglu hyd at y man dinistrio. Gellir ond trosglwyddo data personol i ddarparwyr gwasanaethau trydydd parti sy'n cytuno i gydymffurfio â'r polisiau a'r gweithdrefnau gofynnol, ag sy'n cytuno i roi mesurau digonol ar waith, yn ôl y gofyn.

Rhaid i chi ddiogelu data trwy sicrhau cyfrinachedd, uniondeb ac argaeledd y data personol, fel a ganlyn:

(h) Mae cyfrinachedd yn golygu mai dim ond pobl sydd angen gwybod ac awdurdodi'r data personol medr gael mynediad ato.

(i) Mae uniondeb yn golygu bod data personol yn gywir ac yn addas at y diben y caiff ei brosesu ar ei gyfer.

(j) Mae argaeledd yn golygu bod defnyddwyr awdurdodedig yn gallu cael mynediad at y data personol pan fydd ei angen arnynt at ddibenion awdurdodedig.

Rhaid i chi gydymffurfio â threfniadau diogelu gweinyddol, corfforol a thechnegol y byddwn yn eu gweithredu a'u cynnal yn unol â'r GDPR a'r safonau perthnasol i ddiogelu data personol.

9.2 Adrodd am Dorri Rheolau Data Personol

Mae'r GDPR yn ei wneud yn ofynnol i reolwyr data hysbysu unrhyw doriad o reolau data personol i'r rheolydd perthnasol ac, mewn rhai achosion, y deiliad data.

Os ydych chi'n gwybod neu'n amau bod toriad rheolau data personol wedi digwydd, peidiwch â cheisio ymchwilio i'r mater eich hun. Cysylltwch â'r DPO yn syth.

10. Cyfyngiad trosglwyddo

Mae'r GDPR yn cyfyngu trosglwyddiadau data i wledydd y tu allan i'r AEE er mwyn sicrhau nad yw lefel y diogelu data a roddir i unigolion gan y GDPR yn cael ei danseilio. Rydych chi'n trosglwyddo data personol sy'n deillio o un wlad ar draws ffiniau pan fyddwch yn trosglwyddo, anfon, gweld neu gael mynediad at y data hwnnw mewn gwlad wahanol neu i wlad arall.

Dim ond os yw un o'r amodau canlynol yn berthnasol y gallwch chi drosglwyddo data personol y tu allan i'r AEE:

(a) bod y Comisiwn Ewropeaidd wedi cyhoeddi penderfyniad yn cadarnhau bod y wlad yr ydym yn trosglwyddo'r data personol iddi yn sicrhau lefel ddigonol o ddiogelwch ar gyfer hawliau a rhyddid deiliaid data;

(b) bod mesurau diogelu priodol yn eu lle fel rheolau corfforaethol rhwymol (*binding corporate rules*, "BCR"), cymalau cytundebol safonol a gymeradwywyd gan y Comisiwn Ewropeaidd, cod ymddygiad cymeradwy neu fecanwaith ardystio, y gellir cael copi ohonno gan y DPO;

(c) bod y deiliad data wedi rhoi caniatâd penodol i'r trosglwyddiad arfaethedig ar ôl cael gwybod am unrhyw risgiau posibl; neu

(ch) bod y trosglwyddiad yn angenrheidiol am un o'r rhesymau eraill a nodir yn y GDPR gan gynnwys perfformiad contract rhyngom ni a'r deiliad data, rhesymau budd y cyhoedd, i sefydlu, ymarfer neu amddiffyn hawliadau cyfreithiol neu i ddiogelu'r buddiannau hanfodol y deiliad data lle mae'n gorfforol neu'n gyfreithiol analluog i roi caniatâd ac, mewn rhai achosion cyfyngedig, am ein diddordeb cyfreithlon.

11. Hawliau a cheisiadau Deiliad Data

Mae gan ddeiliaid data hawliau pan ddaw'n fater o sut yr ydym yn trin eu data personol. Mae'r rhain yn cynnwys hawliau i:

(a) tynnu yn ei ôl caniatâd i brosesu ar unrhyw adeg;

(b) dderbyn gwybodaeth benodol am weithgareddau prosesu rheolwr data;

(c) gofyn am fynediad at y data personol yr ydym yn ei gadw amdanynt;

(ch) atal ein defnydd o'u data personol at ddibenion marchnata uniongyrchol;

(d) gofyn i ni ddileu data personol os nad yw bellach yn angenrheidiol mewn perthynas â'r dibenion y cafodd ei gasglu neu ei brosesu neu i gywiro data anghywir neu i gwblhau data anghyflawn;

(dd) cyfyngu prosesu mewn amgylchiadau penodol;

(e) herio prosesu sydd wedi'i gyfiawnhau ar sail ein buddiannau cyfreithlon neu er budd y cyhoedd;

(f) gofyn am gopi o'r cytundeb sy'n caniatáu'r trosglwyddiad o ddata personol y tu allan i'r AEE;

(ff) gwrthwynebu penderfyniadau a wnaed yn seiliedig ar brosesu awtomatig yn unig, gan gynnwys proffilio;

(g) atal prosesu sy'n debygol o achosi difrod neu ofid i'r deiliad data neu unrhyw un arall;

(ng) cael gwybod am dorri rheolau data personol sy'n debygol o arwain at risg uchel i'w hawliau a'u rhyddid;

(h) gwyno i'r awdurdod goruchwylio; a

(i) mewn amgylchiadau cyfyngedig, derbyn neu'n gofyn am drosglwyddo eu data personol i drydydd parti mewn fformat cyffredin ei ddefnydd a strwythuredig.

Rhaid i chi wirio hunaniaeth unigolyn sy'n gofyn am ddata o dan unrhyw un o'r hawliau a restrir uchod (peidiwch â gadael i drydydd partïon eich perswadio i ddatgelu data personol heb awdurdodiad priodol).

Rhaid i chi anfon unrhyw gais deiliad data a gewch i'r Cyfarwyddwr Adnoddau Dynol ar unwaith. Nodwch ei bod yn drosedd cuddio neu ddinistrio data personol sy'n rhan o gais mynediad deiliad data. Byddai ymddygiad o'r fath hefyd yn golygu camymddwyn difrifol o dan ein gweithdrefn ddisgyblu, a allai arwain at eich diswyddiad.

12. Atebolrwydd

12.1 Mae gennym adnoddau a rheolaethau digonol ar waith i sicrhau a dogfennu ein cydymffurfiaeth â GDPR, gan gynnwys:

(a) penodi DPO â chymwysterau addas (lle bo angen) a gweithredwr sy'n atebol am breifatrwydd data;

(b) gweithredu preifatrwydd trwy gynllun wrth brosesu data personol a chwblhau Asesiad Effaith Diogelu Data ("DPIA") lle mae prosesu yn cyflwyno risg uchel i hawliau a rhyddid deiliaid data;

(c) integreiddio diogelu data mewn dogfennau mewnol gan gynnwys y polisi diogelu data hwn;

(ch) hyfforddi ein personél ar y GDPR; ac

(e) yn profi'r mesurau preifatrwydd a weithredir yn rheolaidd ac yn cynnal adolygiadau ac archwiliadau cyfnodol i asesu cydymffurfiaeth, gan gynnwys defnyddio canlyniadau profion i ddangos ymdrech i wella cydymffurfiaeth.

12.2 Cadw cofnodion

Mae'r GDPR yn ei wneud yn ofynnol inni gadw cofnodion llawn a chywir o'n holl weithgareddau prosesu data.

Rhaid i chi gadw cofnodion corfforaethol cywir sy'n adlewyrchu ein prosesu, gan gynnwys cofnodion o ganiatâd deiliaid data a gweithdrefnau ar gyfer derbyn caniatad.

12.3 Archwiliad

Rhaid i chi adolygu'r holl systemau a phrosesau o dan eich rheolaeth yn rheolaidd i sicrhau eu bod yn cydymffurfio â'r polisi diogelu data hwn ac yn gwirio bod rheolaethau ac adnoddau llywodraethu digonol ar waith i sicrhau defnydd gywir a diogeledd data personol.

12.4 Preifatrwydd Drwy Gynllun ac Asesiad Risg Gwarchod Data (DPIA)

Mae'n ofynnol i ni weithredu mesurau preifatrwydd trwy gynllun wrth brosesu data personol trwy weithredu mesurau technegol a threfniadol priodol effeithlon (fel ffugenwi), i sicrhau cydymffurfiaeth ag egwyddorion preifatrwydd data.

Rhaid i chi asesu pa fesurau preifatrwydd trwy gynllun y gellir eu gweithredu ar bob rhaglen / system / proses sy'n prosesu data personol trwy gymryd i ystyriaeth y canlynol:

(a) y ffyrdd fwyaf cyfredol o wneud hynny;

(b) cost gweithredu;

(c) natur, cwmpas, cyd-destun a dibenion y prosesu; a

(ch) y risgiau a'r difrifoldeb mae'r prosesu yn achosi yn erbyn hawliau a rhyddid deiliaid data.

Dylech gynnal DPIA (a thrafod eich canfyddiadau gyda'r DPO) wrth weithredu rhaglenni mawr neu raglenni newid busnes sy'n cynnwys prosesu data personol gan gynnwys:

(d) defnyddio technolegau newydd (rhaglenni, systemau neu brosesau), neu dechnolegau sy'n newid (rhaglenni, systemau neu brosesau);

(f) prosesu awtomatig gan gynnwys proffilio;

(g) prosesu data sensitif ar raddfa fawr; a

(f) monitro systematig ar faes sy'n hygyrch i'r cyhoedd ar raddfa fawr.

12.5 Marchnata uniongyrchol

Rydym yn ddarostyngedig i reolau penodol a chyfreithiau preifat wrth farchnata i'n cwsmeriaid.

Er enghraifft, mae angen caniatâd blaenorol deiliad data ar gyfer marchnata uniongyrchol electronig (er enghraifft, trwy e-bost, testun neu alwadau awtomatig). Mae yna eithriad cyfyngedig i gwsmeriaid presennol a elwir yn "*soft opt in*" yn caniatáu i sefydliadau anfon negeseuon marchnata neu negeseuon e-bost os ydynt wedi cael manylion cyswllt wrth ddarparu gwasanaeth i'r person hwnnw, lle bont yn marchnata cynhyrchion neu wasanaethau tebyg, ac fe roddwyd y cyfle i berson optio allan o'r marchnata wrth gasglu'r manylion yn gyntaf ac ym mhob neges ddilynol.

Rhaid i'r hawl i wrthwynebu marchnata uniongyrchol gael ei gynnig yn benodol i'r deiliad data mewn ffordd ddeallus fel y gellir ei wahaniaethu'n glir o wybodaeth arall.

Rhaid anrhydeddu gwrthwynebiad deiliad data i farchnata uniongyrchol. Os bydd cwsmer yn dewis dod allan ar unrhyw adeg, dylid atal eu manylion cyn gynted ag y bo modd. Mae atal yn golygu cadw ond ychydig o wybodaeth i sicrhau eich bod yn medru parchu dewisiadau marchnata yr unigolyn yn y dyfodol.

12.6 Rhannu Data Personol

Yn gyffredinol, ni chaniateir i ni rannu data personol gyda thrydydd partion oni bai fod rhai mesurau diogelu a threfniadau cytundebol wedi'u sefydlu.

Gellir ond rhannu y data personol sydd gennym gyda gweithiwr arall, asiant neu gynrychiolydd ein grŵp os oes gan y derbynnydd angen cysylltiedig â'i swydd i wybod y wybodaeth ac mae'r trosglwyddiad yn cydymffurfio ag unrhyw gyfyngiadau trosglwyddo trawsffiniol perthnasol.

Gellir ond rhannu'r data personol sydd gennym gyda thrydydd parti, fel ein darparwyr gwasanaeth, os:

(a) oes angen iddynt wybod y wybodaeth at ddibenion darparu'r gwasanaethau dan gontract;

(b) bod rhannu'r data personol yn cydymffurfio â'r rhybudd preifatrwydd a ddarperir i'r deiliad data ac, os oes angen, mae caniatâd y deiliad data wedi'i gael;

(c) bod y trydydd parti wedi cytuno i gydymffurfio â'r safonau diogelwch, polisiau a gweithdrefnau gofynnol a rhoi mesurau diogelwch digonol ar waith;

(ch) bod y trosglwyddiad yn cydymffurfio ag unrhyw gyfyngiadau trosglwyddo trawsffiniol perthnasol; a

(d) bod cytundeb ysgrifenedig llawn sy'n cynnwys cymalau trydydd parti a gymeradwywyd gan GDPR wedi'i sicrhau.

13. Newidiadau i'r Polisi Diogelu Data hwn

Rydym yn cadw'r hawl i newid y polisi diogelu data hwn ar unrhyw adeg felly gwiriwch yn ôl yn rheolaidd i gael y copi diweddaraf o'r polisi diogelu data hwn.