POLISI DIOGELU DATA

Fersiwn 4

Cyhoeddwyd: Rhagfyr 2021

POLISI DIOGELU DATA URDD GOBAITH Cymru

1. Cyflwyniad

1.1 Mae'r Urdd yn dal data personol am y rheiny sy'n gwneud cais am swyddi, cyflogeion, gweithwyr, gwirfoddolwyr, cwsmeriaid, aelodau a'u rhieni, cyflenwyr, prentisiaid a dysgwyr ac unigolion eraill ar gyfer amrywiaeth o ddibenion sefydliadol.

1.2 Mae'r Urdd yn cydnabod y bydd ymdrin â data personol mewn modd addas a chyfreithlon yn sicrhau bod gan bobl hyder yn y sefydliad ac yn caniatáu i'r sefydliad weithredu'n llwyddiannus. Mae diogelu cyfrinachedd ac uniondeb data personol yn gyfrifoldeb hollbwysig yr ydym yn ei gymryd o ddifrif bob amser.

1.3 Mae'r polisi hwn yn nodi sut mae'r Urdd yn ceisio diogelu data personol a sicrhau bod staff a gwirfoddolwyr yn deall y rheolau sy'n effeithio ar eu defnydd o ddata personol y mae ganddynt fynediad iddo yn rhan o'u gwaith.

1.4 Mae'r polisi hwn yn berthnasol i'r holl ddata personol y mae'r Urdd yn ei brosesu, waeth pa gyfrwng sy'n cael ei ddefnyddio i storio'r data hwnnw, a waeth pwy y mae'n ymwneud â hwy, boed y rheiny'n gyflogeion, gweithwyr, gwirfoddolwyr, cwsmeriaid, aelodau a'u rhieni, cyflenwyr neu unrhyw unigolion eraill, yn y gorffennol neu'r presennol.

1.5 Mae'r polisi hwn yn ei gwneud yn ofynnol i staff a gwirfoddolwyr sicrhau eu bod yn ymgynghori â'r Rheolwr Preifatrwydd Data cyn dechrau ar unrhyw weithgaredd prosesu data newydd sylweddol er mwyn sicrhau bod camau cydymffurfio perthnasol yn cael sylw.

1.6 Y Rheolwr Preifatrwydd Data sy'n gyfrifol am fonitro a gweithredu'r polisi hwn. Os oes gennych unrhyw gwestiynau am gynnwys y polisi hwn neu unrhyw sylwadau eraill, dylech gysylltu â'r Rheolwr Preifatrwydd Data. Yn benodol, **rhaid** i staff a gwirfoddolwyr gysylltu â'r Rheolwr Preifatrwydd Data **bob tro** yn yr amgylchiadau canlynol:

(a) Nid yw'n eglur pa sail gyfreithiol y dylid dibynnu arni wrth brosesu data personol (gan gynnwys y buddiannau dilys sy'n cael eu defnyddio gan yr Urdd (gweler adran 5.2 isod));

(b) Mae angen dibynnu ar ganiatâd a / neu ganiatâd eglur i brosesu data personol (gweler adran 14 isod);

(c) Mae angen drafftio hysbysiad preifatrwydd (gweler adran 5.7 isod);

(d) Os yw hyd y cyfnod cadw ar gyfer y data personol sy'n cael ei brosesu yn aneglur neu'n anhysbys (gweler adran 9 isod);

(e) Nid yw'n glir pa ddiogelwch neu fesurau eraill sydd angen eu gweithredu i ddiogelu data personol (gweler adran 10 isod);

(f) Mae data personol yn cael ei drosglwyddo y tu allan i'r AEE (gweler adran15 isod);

(g) Os oes achos o dorcyfraith mewn perthynas â data personol wedi digwydd (adran 19 isod);

(h) Pryd bynnag y bydd newid sylweddol mewn gweithgarwch prosesu neu pan fydd gweithgarwch prosesu newydd mewn perthynas â data personol (efallai y bydd angen Asesiad Effaith Diogelu Data) (gweler adran 13 isod);

(i) Mewn achos lle'r bwriad yw defnyddio data personol at ddiben gwahanol i'r diben y cafodd y data ei gasglu'n wreiddiol.

2. Cwmpas

2.1 Mae'r polisi hwn yn berthnasol i holl staff yr Urdd. At y dibenion hyn, mae'r holl staff yn cynnwys cyflogeion, gweithwyr dros dro a gweithwyr asiantaeth, contractwyr eraill, internwyr a gwirfoddolwyr.

2.2 Rhaid i'r holl staff fod yn gyfarwydd â'r polisi hwn a chydymffurfio â'i delerau.

2.3 Mae cydymffurfio â'r polisi hwn yn orfodol. Rhaid i staff hefyd gydymffurfio ag unrhyw bolisïau cysylltiedig a hysbysiadau preifatrwydd. Gall unrhyw achos o beidio â chydymffurfio â'r Polisi Diogelu Data hwn arwain at gamau disgyblu.

2.4 Gall yr Urdd ddiwygio'r polisi hwn, neu ychwanegu ato, gyda pholisïau a chanllawiau ychwanegol o dro i dro.

3. Diffiniadau

3.1 Yn y polisi hwn:

(a) **Data personol** yw gwybodaeth sy'n ymwneud ag unigolion mae modd eu hadnabod, fel ymgeiswyr am swyddi, cyflogeion presennol a chyn-gyflogeion, gwirfoddolwyr, gweithwyr asiantaeth a gweithwyr contract y presennol a'r gorffennol, staff eraill, aelodau a'u rhieni, cyflenwyr a chysylltiadau marchnata. Mae hyn yn cynnwys mynegi barn am yr unigolyn ac unrhyw arwydd o fwriadau rhywun arall tuag at yr unigolyn.

(b) **Data personol categori arbennig** yw gwybodaeth sy'n datgelu tarddiad hiliol neu ethnig, barn wleidyddol, credoau crefyddol neu debyg, aelodaeth o undeb llafur, cyflyrau iechyd corfforol neu feddyliol, bywyd rhywiol, tuedd rywiol, data biometrig neu enetig. Dylid trin data personol sy'n ymwneud â throseddau ac euogfarnau hefyd fel data personol categori arbennig.

(c) **Prosesu data** yw unrhyw weithgarwch sy'n cynnwys defnyddio data personol. Mae'n cynnwys cael, cofnodi neu ddal y data, neu gyflawni unrhyw weithrediad neu set o weithrediadau gan ddefnyddio'r data gan gynnwys ei drefnu, ei ddiwygio, ei adfer, ei ddefnyddio, ei ddatgelu, ei ddileu neu ei ddinistrio. Mae prosesu hefyd yn cynnwys trosglwyddo data personol i drydydd partïon.

4. Egwyddorion Cyffredinol

4.1 Polisi'r Urdd yw prosesu data personol yn unol â chyfreithiau diogelu data perthnasol a hawliau unigolion fel sydd wedi'u nodi isod. Mae gan yr holl staff gyfrifoldeb personol i gymhwyso Polisi Diogelu Data yr Urdd yn ymarferol.

4.2 Bydd yr Urdd yn dilyn yr egwyddorion canlynol mewn perthynas â phrosesu data personol, gan sicrhau bod data personol:

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

(b) Yn cael ei gasglu at ddibenion penodol, eglur a chyfreithlon yn unig ('Cyfyngiad Pwrpas')

(c) Yn ddigonol, yn berthnasol ac wedi'i gyfyngu i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y caiff ei brosesu ar eu cyfer ('Minimeiddio Data').

(d) Yn gywir ac yn cael ei ddiweddaru yn ôl yr angen ('Cywirdeb').

(e) Heb ei gadw ar ffurf sy'n caniatáu adnabod unigolion am gyfnod hwy nag sy'n angenrheidiol at y dibenion y mae'r data'n cael ei brosesu ar eu cyfer ('Cyfyngiad Storio').

(f) Wedi'i brosesu mewn modd sy'n sicrhau ei ddiogelwch gan ddefnyddio mesurau technegol a threfniadol priodol i'w ddiogelu rhag prosesu anawdurdodedig neu anghyfreithlon, ac yn erbyn ei golli, ei ddinistrio neu'i ddifrodi'n ddamweiniol ('Diogelwch, Uniondeb a Chyfrinachedd').

4.3 Mae'r Urdd yn gyfrifol am gydymffurfio â'r egwyddorion diogelu data sydd wedi'u rhestru uchod, a rhaid iddo allu dangos y gydymffurfiaeth honno ('Egwyddor Atebolrwydd').

5. Cyfreithlondeb, Tegwch a Thryloywder

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

Cyfreithlondeb

5.2 Dylai staff sicrhau bod sail gyfreithiol ar gyfer prosesu data personol. Mae'r seiliau cyfreithiol ar gyfer prosesu fel a ganlyn:

(a) mae'r unigolyn wedi rhoi ei ganiatâd (gweler 14 isod);

(b) mae angen prosesu'r data er mwyn cyflawni contract â'r unigolyn;

(c) bodloni rhwymedigaethau cydymffurfio cyfreithiol yr Urdd;

(d) diogelu buddiannau hanfodol yr unigolyn;

(e) cyflawni tasg er budd y cyhoedd;

(f) cynnal buddiannau cyfreithlon yr Urdd, lle na chaiff y buddiannau hyn eu diystyru oherwydd bod y prosesu yn rhagfarnu yn erbyn buddiannau

neu hawliau a rhyddid sylfaenol yr unigolyn/unigolion. Mae rhaid i'r hysbysiadau preifatrwydd nodi'r dibenion sy'n cyfrif fel buddiannau cyfreithlon y byddwn ni'n prosesu data ar eu cyfer (gweler adran 5.7 isod).

5.3 Os nad yw staff yn siŵr pa sail gyfreithiol sy'n berthnasol i'r data personol y maent yn ei brosesu, dylent gysylltu â'r Rheolwr Preifatrwydd Data.

5.4 Mae data personol categori arbennig (gweler 3.1(b) uchod) yn gofyn am lefelau uwch o ddiogelwch a sail gyfreithiol arall yn ychwanegol at y rhai sy wedi'u hamlinellu yn adran 5.2 er mwyn ei brosesu'n gyfreithlon.

5.5 Fel arfer, caniatâd *eglur* yr unigolyn fydd y sail gyfreithiol ychwanegol briodol ar gyfer prosesu data personol categori arbennig mewn perthynas ag aelodau. Dylai staff gysylltu â'r Rheolwr Preifatrwydd Data am ragor o wybodaeth am y sail gyfreithiol briodol ar gyfer prosesu data categori arbennig.

5.6 Bydd yr Urdd hefyd yn prosesu data personol categori arbennig mewn perthynas â'i staff. Y sail gyfreithiol ychwanegol ar gyfer prosesu data personol categori arbennig staff fel rheol yw ei bod yn angenrheidiol at ddibenion cyflawni rhwymedigaethau ac arfer hawliau penodol ym maes cyfraith cyflogaeth. Sail gyfreithiol arall yw bod prosesu'r data hwn yn angenrheidiol am resymau o fudd sylweddol i'r cyhoedd, er enghraifft monitro cydraddoldeb, atal neu ganfod gweithredoedd anghyfreithlon, amddiffyn y cyhoedd rhag anonestrwydd, diogelu, atal twyll neu amheuaeth o derfysgaeth neu wyngalchu arian. Dylai staff gysylltu â'r Rheolwr Preifatrwydd Data am ragor o wybodaeth am y sail gyfreithiol briodol ar gyfer prosesu data categori arbennig. Yn ogystal â hyn, dylai staff roi sylw arbennig i adran 12 isod.

Tegwch a Thryloywder (Hysbysiadau Preifatrwydd)

5.7 Mae cyfraith diogelu data yn ei gwneud yn ofynnol i ni ddarparu gwybodaeth fanwl, benodol i unigolion ynghylch sut a pham y mae eu data personol yn cael ei brosesu. Rhaid darparu gwybodaeth o'r fath trwy hysbysiadau preifatrwydd priodol.

5.8 Rhaid i hysbysiadau preifatrwydd fod yn gryno, yn dryloyw, yn ddealladwy, yn hygyrch, ac mewn iaith glir a phriodol fel y gall unigolyn eu deall yn hawdd.

5.9 Pryd bynnag y bydd yr Urdd yn casglu data personol yn uniongyrchol wrth unigolyn, rhaid darparu, neu gyfeirio'r unigolyn at, yr hysbysiad preifatrwydd sy'n cynnwys yr holl wybodaeth sy'n ofynnol yn ôl cyfraith diogelu data (gan gynnwys nodi pwy yw rheolwr y data, sut a pham y bydd yr Urdd yn defnyddio'r data personol hwnnw, ei brosesu, ei ddatgelu, ei amddiffyn a'i gadw). Bydd yr hysbysiad preifatrwydd hefyd yn ei gwneud yn glir ar ba sail gyfreithiol y mae'r Urdd yn dibynnu a'r sail gyfreithiol briodol ychwanegol os yw data personol categori arbennig yn cael ei brosesu. Rhaid darparu'r hysbysiad preifatrwydd pan fydd yr unigolyn yn rhoi data personol i'r Urdd am y tro cyntaf. Fel rheol, bydd rhybudd preifatrwydd cyffredinol yr Urdd yn briodol mewn perthynas â'r dibenion sefydliadol cyffredinol y mae'r Urdd yn casglu data personol ar eu cyfer. Dylai staff roi dolen i'r unigolyn neu gyfarwyddo'r unigolyn i'r hysbysiad preifatrwydd hwn ar y pwynt y bydd y data personol yn cael ei gasglu. Mae hwn ar gael ar wefan yr Urdd.

5.10 Pan gaiff data personol ei gasglu'n anuniongyrchol (er enghraifft, gan drydydd parti neu ffynhonnell sydd ar gael i'r cyhoedd), rhaid rhoi hysbysiad preifatrwydd i'r unigolyn sy'n cynnwys yr holl wybodaeth sy'n ofynnol dan y gyfraith diogelu data, cyn gynted ag y bo modd, ar ôl casglu / derbyn y data. Ni ddylai'r hysbysiad preifatrwydd gael ei ddarparu i'r unigolyn yn hwyrach na'r cyfathrebiad cyntaf gyda'r unigolyn neu 1 mis o dderbyn y data personol (pa un bynnag sydd gynharach), oni bai bod hyn yn amhosibl neu'n gofyn am ymdrech anghymesur.

5.11 Fel sydd wedi'i nodi yn adran 5.9 uchod, fel rheol bydd hysbysiad preifatrwydd cyffredinol yr Urdd yn briodol mewn perthynas â'r dibenion sefydliadol cyffredinol y mae'r Urdd yn casglu data personol ar eu cyfer. Dylai staff roi dolen i'r unigolyn neu gyfarwyddo'r unigolyn i'r hysbysiad preifatrwydd hwn yn y cyfathrebiad cyntaf neu o fewn 1 mis o dderbyn y data personol, pa un bynnag sydd gynharach. Fel arfer mae modd cyflawni hyn trwy gynnwys y ddolen i'r hysbysiad preifatrwydd yn y llofnod e-bost. Dylai staff hysbysu'r Rheolwr Preifatrwydd Data os yw hyn yn debygol o fod yn amhosibl neu'n cynnwys ymdrech anghymesur.

5.12 Mae'n ofynnol i staff gynnwys dolen i hysbysiad preifatrwydd yr Urdd yn eu llofnod e-bost.

5.13 Dylai staff gysylltu â'r Rheolwr Preifatrwydd Data os oes angen drafftio hysbysiad preifatrwydd neu os nad ydynt yn sicr pryd y mae angen hysbysiad preifatrwydd.

6. Cyfyngiad pwrpas

6.1 Rhaid casglu data personol at ddibenion penodol, eglur a chyfreithlon yn unig. Ni ddylai data gael ei brosesu ymhellach mewn unrhyw fodd nad yw'n cyd-fynd â'r dibenion hynny.

6.2 Ni all staff ddefnyddio data personol ar gyfer dibenion newydd, neu ddibenion gwahanol i'r rhai a gafodd eu datgelu pan gafwyd y data personol yn gyntaf, neu at ddibenion nad ydynt yn cyd-fynd â'r rheiny a gafodd eu datgelu bryd hynny. Mae hyn yn wir oni bai bod y staff wedi hysbysu'r unigolion o'r dibenion a'r sail gyfreithiol newydd maent yn dibynnu arnynt (os yw'r sail gyfreithiol hon yn ganiatâd, rhaid cael cydsyniad priodol (gweler adran 14 isod).

7. Minimeiddio data

7.1 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 eu cyfer.

7.2 Caiff staff brosesu data personol pan maent yn cyflawni dyletswyddau eu gwaith yn unig. Ni ddylid casglu data personol gormodol a dylai staff sicrhau, hyd eithaf eu gallu, fod unrhyw ddata personol sy'n cael ei gasglu yn ddigonol ac yn berthnasol i'r dibenion maen nhw'n bwriadu ei ddefnyddio ar eu cyfer.

7.3 Rhaid i staff sicrhau eu bod yn dileu data neu eu wneud yn ddienw yn unol â Pholisi Cadw Dogfennau, Data ac Archifau'r Urdd pan na fydd angen y data personol at y dibenion sydd wedi'u nodi mwyach.

8. Cywirdeb

8.1 Rhaid i ddata personol fod yn gywir, a rhaid ei ddiweddaru'n gyson yn ôl yr angen. Rhaid ei gywiro neu ei ddileu heb oedi pan fydd yn anghywir.

8.2 Bydd staff yn sicrhau bod y data personol y mae'r Urdd yn ei ddefnyddio a'i ddal yn gywir, yn gyflawn, wedi'i ddiweddaru ac yn berthnasol i'r diben y cafodd ei gasglu ar ei gyfer. Rhaid i'r staff wirio cywirdeb unrhyw ddata personol wrth ei gasglu, ac yn rheolaidd ar ôl hynny. Rhaid i staff gymryd pob cam rhesymol i ddinistrio neu ddiwygio data personol anghywir neu ddata personol sydd wedi dyddio.

8.3 Rhaid i staff sicrhau bod y data personol mae'r Urdd yn ei ddal amdanynt hwy yn gywir ac yn cael ei ddiweddaru yn ôl yr angen. Os yw manylion personol neu amgylchiadau yn newid, dylai staff roi gwybod i'r adran Adnoddau Dynol, fel bod modd diweddaru cofnodion yr Urdd.

9. Cyfyngiad storio (cadw data)

9.1 Ni ddylai Data Personol gael ei gadw ar ffurf lle mae modd adnabod yr unigolyn am gyfnod hwy nag sy'n angenrheidiol at y dibenion y mae'r data'n cael ei brosesu ar eu cyfer.

9.2 Rhaid i staff beidio â chadw data personol, ar ffurf sy'n caniatáu adnabod unigolyn, am gyfnod hwy nag sydd ei angen ar gyfer y diben neu ddibenion cyfreithlon y gwnaeth yr Urdd gasglu'r data ar eu cyfer yn wreiddiol.

9.3 Mae gan yr Urdd gyfnodau cadw data penodol i sicrhau bod data personol yn cael ei ddileu, ar ôl amser rhesymol, pan nad oes ei angen mwyach at y dibenion yr oedd yn cael ei ddal ar eu cyfer.

9.4 Bydd staff yn cymryd pob cam rhesymol i ddinistrio'r holl ddata personol nad oes ei angen rhagor, neu ei ddileu o systemau'r Urdd, yn unol â Chyfnodau Cadw Data'r Urdd. Mae hyn yn cynnwys ei gwneud yn ofynnol i drydydd partïon ddileu data o'r fath lle bo'n briodol.

9.5 Bydd staff yn sicrhau bod unigolion yn cael gwybod am ba hyd y bydd eu data'n cael eu storio, a sut mae hyd y cyfnod hwnnw wedi'i bennu, yn yr hysbysiadau preifatrwydd perthnasol (gweler adrannau 5.7 - 5.13).

10. Diogelwch, uniondeb a chyfrinachedd

10.1 Rhaid diogelu data personol trwy fesurau technegol a threfniadol priodol yn erbyn prosesu anawdurdodedig neu anghyfreithlon, ac yn erbyn ei golli, ei ddinistrio neu'i ddifrodi'n ddamweiniol.

10.2 Rhaid i'r Urdd weithredu mesurau diogelwch rhesymol a phriodol yn erbyn prosesu data personol mewn modd anghyfreithlon neu anawdurdodedig ac yn erbyn colli data, neu'i ddifrodi neu'i ddinistrio'n ddamweiniol.

10.3 Rhaid i'r Urdd gynnal diogelwch data trwy ddiogelu cyfrinachedd, uniondeb ac argaeledd y data personol, a gaiff eu diffinio fel a ganlyn:

(a) Mae cyfrinachedd yn golygu bydd mynediad i'r data ar gael i'r rheiny sydd angen gwybod ac sydd wedi'u hawdurdodi i'w weld yn unig.

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

(c) Mae argaeledd yn golygu bod defnyddwyr awdurdodedig yn gallu cael mynediad at y data personol pan fydd ei angen ar gyfer dibenion awdurdodedig.

10.4 Bydd yr Urdd yn datblygu, gweithredu a chynnal mesurau diogelu sy'n briodol ar gyfer:

(a) ein maint, ein cwmpas a'n busnes;

(b) ein hadnoddau sydd ar gael;

(c) faint o ddata personol rydym yn berchen arno neu'n ei gynnal ar ran eraill; a

(d) risgiau sydd wedi'u hadnabod (gan gynnwys defnyddio prosesau amgryptio a ffugenwi (h.y. disodli gwybodaeth sy'n caniatáu adnabod unigolyn yn uniongyrchol neu'n anuniongyrchol gydag un neu ragor o arwyddion neu ffugenwau artiffisial, fel nad oes modd adnabod y person y mae'r data yn ymwneud ag ef/hi, heb ddefnyddio gwybodaeth ychwanegol sydd i'w chadw ar wahân ac yn ddiogel) lle bo'n berthnasol).

10.5 Bydd yr Urdd yn gwerthuso'r mesurau diogelu hynny yn rheolaidd, a phrofi eu heffeithiolrwydd, i sicrhau diogelwch ein gweithgareddau prosesu data personol.

10.6 Mae gan staff gyfrifoldeb dros ddiogelu'r data personol mae'r Urdd yn ei ddal.

10.7 Rhaid i staff weithredu â gofal penodol wrth ddiogelu data personol categori arbennig (gweler 3.1(b) uchod) rhag cael ei golli, neu rhag i rywun ei weld, ei ddefnyddio neu'i ddatgelu heb awdurdod.

10.8 Rhaid i staff ddilyn yr holl weithdrefnau mae'r Urdd wedi'u rhoi ar waith i gynnal diogelwch yr holl ddata personol o'r pwynt lle y caiff ei gasglu i'r pwynt lle y caiff ei ddinistrio. Gall staff drosglwyddo data personol dim ond i ddarparwyr gwasanaeth trydydd parti sy'n cytuno i gydymffurfio â'r polisïau a'r gweithdrefnau gofynnol ac sy'n cytuno i roi mesurau digonol yn eu lle, yn ôl y gofyn (gweler adrannau 15 a 16 isod).

10.9 Rhaid i staff gydymffurfio â systemau diogelu gweinyddol, corfforol a thechnegol sy'n cael eu gweithredu a'u cynnal yn unol â chyfraith diogelu data a safonau perthnasol i ddiogelu data personol. Ni ddylai staff ymdrechu i osgoi'r systemau hyn.

11. Atebolrwydd

11.1 Rhaid i'r Urdd roi mesurau technegol a threfniadol priodol ar waith i sicrhau cydymffurfio ag egwyddorion diogelu data (sydd wedi'u nodi yn adran 4.2 uchod). Mae'r Urdd yn gyfrifol am gydymffurfio â'r egwyddorion diogelu data, ac mae'n rhaid i'r sefydliad allu dangos ei fod yn cydymffurfio â hwy.

11.2 Rhaid i'r Urdd roi adnoddau a rheolaethau digonol yn eu lle i sicrhau a chofnodi cydymffurfio â deddfau diogelu data, gan gynnwys:

(a) penodi rheolwr preifatrwydd data sy'n gyfrifol am gydymffurfio â chyfraith diogelu data;

(b) gwreiddio diogelu data o'r cychwyn ac fel anghenraid wrth brosesu data personol i sicrhau cydymffurfio â chyfreithiau diogelu data perthnasol (gweler adran 13 isod);

(c) cwblhau Asesiadau Effaith Diogelu Data (DPIAs) i nodi a lleihau risgiau gweithgaredd prosesu data, lle mae prosesu yn peri risg uchel i hawliau a rhyddid unigolion. Dylid cynnal DPIAs ar gyfer pob rhaglen newid system sylweddol neu raglen newid busnes sylweddol sy'n ymwneud â phrosesu data personol, yn arbennig y rhai sy'n cynnwys mentrau neu dechnoleg newydd (gweler adran 13 isod);

(d) integreiddio diogelu data i ddogfennau mewnol, polisïau a gweithdrefnau gan gynnwys y Polisi Diogelu Data hwn;

(e) hyfforddi staff yn rheolaidd ar gyfraith diogelu data berthnasol, y Polisi Diogelu Data hwn, polisïau cysylltiedig a materion diogelu data, gan gynnwys, er enghraifft, hawliau unigol, caniatâd, sail gyfreithiol, DPIAs ac achosion o dorcyfraith yn ymwneud â data personol; a

(f) rhoi'r mesurau preifatrwydd sy'n cael eu gweithredu ar brawf yn rheolaidd a chynnal adolygiadau ac archwiliadau cyfnodol i asesu cydymffurfiaeth, gan gynnwys defnyddio canlyniadau profion i ddangos ymdrech i wella cydymffurfiaeth.

12. Data Personol Categori Arbennig

12.1 Oherwydd y sensitifrwydd penodol o ran prosesu data personol categori arbennig, mae Deddf Diogelu Data 2018 yn mynnu bod gan yr Urdd ddogfennaeth bolisi yn ei le i esbonio gweithdrefnau'r Urdd ar gyfer sicrhau cydymffurfio â'r egwyddorion diogelu data (gweler adran 4.2) ac i esbonio polisïau'r Urdd o ran cadw a dileu'r data personol categori arbennig (adran 9 uchod).

12.2 Yn unol â hynny, wrth brosesu data personol categori arbennig, yn ogystal â'r materion sydd wedi'u nodi yn adrannau 5-11 uchod, rhaid hefyd ystyried y materion sydd wedi'u nodi isod.

Data Personol Categori Arbennig

12.3 Wrth brosesu data personol categori arbennig staff, naill ai gan ddibynnu ar y sail gyfreithiol bod y prosesu yn angenrheidiol at ddibenion cyflawni'r rhwymedigaethau ac arfer hawliau penodol ym maes cyfraith cyflogaeth neu, gan ddibynnu ar fudd cyhoeddus sylweddol fel sail, rhaid rhoi ystyriaeth benodol i:

(a) sicrhau bod y data personol categori arbennig yn cael ei rannu'n fewnol yn unig gydag unigolion sydd angen gwybod yr wybodaeth. Fel arfer bydd hyn yn golygu rhannu'r wybodaeth â'r adran Adnoddau Dynol a rheolwr llinell yr aelod o staff. Dylid meddwl yn ofalus cyn

rhannu'r data hwn ymhellach yn fewnol a dylid gofyn am arweiniad gan y Rheolwr Preifatrwydd Data;

(b) ystyried a yw'n ymarferol i wneud y data'n ddienw, er enghraifft wrth brosesu data personol categori arbennig ar gyfer monitro cyfleoedd cyfartal;

(c) maint y data personol categori arbennig sy'n cael ei gadw, [er enghraifft gyda gwiriadau'r Gwasanaeth Datgelu a Gwahardd ('DBS') sy'n cael eu hystyried yn foddhaol gan yr Urdd, mae cofnodi'r ffaith bod gwiriad DBS wedi'i gynnal ar ddyddiad penodol a bod y canlyniadau'n foddhaol yn ddigon – dyna'r holl wybodaeth sydd angen ei chadw. Mae hyn yn sicrhau na chaiff data personol categori arbennig ei gadw. Pan fo canlyniad y gwiriad DBS yn cael ei ystyried yn anfoddhaol gan yr Urdd, ni ddylai canlyniad yr gwiriad gael ei gadw am gyfnod hwy nag sy'n angenrheidiol, gweler Polisi Cadw Dogfennau, Data ac Archifau a Polisi Trefniadau Gweinyddol GDG ac ni ddylai gael ei gadw am gyfnod hwy na 6 mis ar unrhyw gyfrif];

(d) Bolisi Cadw Dogfennau, Data ac Archifau yr Urdd gan y bydd gan rai mathau o ddata personol categori arbennig gyfnodau cadw byrrach penodol. Dylid cymryd gofal penodol i sicrhau eich bod yn glynu wrth y cyfnodau cadw sydd wedi'u pennu ar gyfer data o'r fath yn amserlen cadw data yr Urdd.

<u>Data Personol Categori Arbennig wedi'i gofnodi gan Deledu Cylch Cyfyng (CCTV)</u>

12.4 Wrth recordio delweddau gan ddefnyddio teledu cylch cyfyng, mae'n bosib y bydd y delweddau sy'n cael eu casglu yn datgelu trosedd sy'n cael ei gyflawni. Mewn amgylchiadau o'r fath efallai y bydd angen trin y delweddau fel data personol categori arbennig. Mewn amgylchiadau o'r fath, mae'n debyg mai'r sail gyfreithiol ar gyfer prosesu'r data personol yw bod y prosesu yn angenrheidiol am resymau o fudd sylweddol i'r cyhoedd, sef atal a chanfod trosedd. Lle mae hyn yn wir, rhaid rhoi ystyriaeth benodol i:

(a) sicrhau bod y data personol yn cael ei rannu'n fewnol yn unig gydag unigolion sydd angen gwybod yr wybodaeth. Fel arfer bydd hyn yn golygu'r cyfarwyddwyr. Dylid meddwl yn ofalus cyn rhannu'r data hwn ymhellach yn fewnol a dylid gofyn am arweiniad gan y Rheolwr Preifatrwydd Data;

(b) sicrhau bod y data personol yn cael ei rannu'n allanol gyda chaniatâd penodol y Rheolwr Preifatrwydd Data yn unig;

(c) datgelu'r ffilm/delwedd ar gais i'r trydydd partïon isod pan fydd y Rheolwr Preifatrwydd Data yn ystyried bod hynny'n briodol ar ôl ystyried yr holl amgylchiadau perthnasol, a phryd hynny'n unig:

(i) I'r heddlu;

(ii) I asiantaethau erlyn;

(iii) I gynrychiolwyr cyfreithiol perthnasol; a/neu

(iv) I bobl y mae eu delweddau wedi'u cofnodi a'u cadw.

(d) lle bo'r delweddau yn ofynnol ar gyfer dibenion tystiolaethol mewn achosion disgyblu cyfreithiol neu gyfundrefnol, bydd recordiad disg DVD yn cael ei wneud a'i osod mewn amlen wedi'i selio, wedi'i llofnodi a'i dyddio, a'i chadw mewn lleoliad diogel gan y Rheolwr Preifatrwydd Data hyd nes y bydd yr ymchwiliad wedi'i gwblhau. Caiff mynediad i'r delweddau hyn ei reoli'n llym.

(e) ar ddiwedd eu hoes ddefnyddiol, bydd yr holl ddelweddau sydd wedi'u cadw ym mha bynnag fformat yn cael eu dileu yn barhaol ac yn ddiogel. Bydd unrhyw ddeunydd, fel tapiau neu ddisgiau, yn cael ei waredu fel gwastraff cyfrinachol. Bydd unrhyw ffotograffau neu brintiau copi caled yn cael eu gwaredu fel gwastraff cyfrinachol.

13. Preifatrwydd o'r Cychwyn ac Asesiadau Effaith Diogelu Data (DPIAs)

13.1 Mae'n ofynnol i'r Urdd wreiddio preifatrwydd o'r cychwyn wrth brosesu data personol trwy weithredu mesurau technegol a threfniadol priodol mewn modd effeithiol, er mwyn sicrhau cydymffurfio ag egwyddorion preifatrwydd data.

13.2 Rhaid i'r Urdd asesu pa fesurau y mae modd eu gwreiddio ar bob rhaglen / system / proses sy'n prosesu data personol er mwyn sicrhau preifatrwydd o'r cychwyn trwy ystyried y canlynol:

(a) defnyddio'r mesurau mwyaf diweddar (h.y. defnyddio'r ddyfais, y weithdrefn, y broses neu'r dechneg fwyaf datblygedig sydd ar gael ar yr adeg honno);

(b) cost gweithredu;

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

(d) y risgiau o debygolrwydd amrywiol sy'n codi wrth brosesu data, a pha mor llym yw effaith y prosesu ar hawliau a rhyddid yr unigolion.

13.3 Rhaid i'r Urdd gynnal Asesiadau Effaith Diogelu Data mewn perthynas â phrosesu sy'n cael ei ystyried yn risg uchel (er enghraifft, pan fo prosesu yn cynnwys data personol categori arbennig ar raddfa fawr).

13.4 Dylai staff gysylltu â'r Rheolwr Preifatrwydd Data a chynnal Asesiad Effaith Diogelu Data wrth weithredu rhaglenni newid system sylweddol neu raglenni newid busnes sylweddol sy'n ymwneud â phrosesu data personol gan gynnwys:

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

(b) prosesu awtomataidd gan gynnwys proffilio a gwneud penderfyniadau awtomataidd;

(c) prosesu data categori arbennig ar raddfa fawr; a

(d) monitro ardal sy'n hygyrch i'r cyhoedd yn systematig ar raddfa fawr (e.e. gan ddefnyddio CCTV).

13.5 Rhaid i Asesiad Effaith Diogelu Data gynnwys:

(a) disgrifiad o'r prosesu, ei ddibenion a buddiannau dilys y rheolwr data os yw'n briodol;

(b) asesiad o angenrheidrwydd a chymesuredd y prosesu mewn perthynas â'i ddiben;

(c) asesiad o'r risg i unigolion; a

(d) y mesurau lliniaru risg sydd yn eu lle a dangos cydymffurfiaeth.

13.6 Mae templed ffurflen Asesiad Effaith Diogelu Data ar gael ar Wefan y Comisiynydd Gwybodaeth.

14. Caniatâd

14.1 Rhaid i'r Urdd sicrhau bod data personol yn cael ei brosesu ar sail un neu ragor o'r seiliau cyfreithiol sydd wedi'u nodi yn adran 5.2 uchod. Un o'r rhain yw caniatâd.

14.2 Er mwyn i unigolyn roi caniatâd dilys i brosesu ei ddata personol, mae rhaid iddo roi'r caniatâd hwnnw'n rhydd, ar gyfer diben penodol. Rhaid iddo fod yn wybodus am y caniatâd mae'n ei roi, a rhaid bod y caniatâd yn arwydd diamwys, trwy ddatganiad neu drwy gamau cadarnhaol clir, o ddymuniad yr unigolyn i gytuno i'w ddata personol gael ei brosesu.

14.3 Mae angen caniatâd *cadarnhaol* felly nid yw tawelwch, bocsys wedi'u ticio ymlaen llaw neu anweithgarwch yn ddigonol.

14.4 Os yw caniatâd yn cael ei roi mewn dogfen sy'n ymdrin â materion eraill, yna rhaid cadw'r caniatâd ar wahân i'r materion eraill hynny.

14.5 Rhaid bod ffordd hawdd i'r unigolyn dynnu ei ganiatâd yn ei ôl a rhaid bodloni'r cais hwnnw yn brydlon. Efallai y bydd angen adnewyddu caniatâd os yw'r Urdd yn bwriadu prosesu data personol ar gyfer diben gwahanol ac anghydnaws na chafodd ei ddatgelu pan roddodd yr unigolyn ei ganiatâd yn y lle cyntaf.

14.6 Ni ddylid dibynnu ar ganiatâd fel sail gyfreithiol ar gyfer prosesu, os yw sail gyfreithiol arall fwy priodol yn berthnasol.

14.7 Ni ddylid dibynnu ar ganiatâd fel arfer lle mae anghydbwysedd yn y berthynas rhwng yr unigolyn a'r Urdd, er enghraifft yng nghyd-destun perthynas cyflogwr / cyflogai.

14.8 Mae angen caniatâd eglur fel arfer ar gyfer:

(a) Prosesu data personol categori arbennig (er dylai staff gysylltu â'r Rheolwr Preifatrwydd Data i benderfynu ar y sail gyfreithiol fwyaf priodol ar gyfer prosesu data categori arbennig).

(b) Gwneud penderfyniadau awtomataidd; a

(c) Trosglwyddo data ar draws ffiniau.

14.9 Mae caniatâd eglur yn gofyn am ddatganiad cydsyniad clir a phenodol iawn gan yr unigolyn (hynny yw, nid gweithredu yn unig) a dylai'r unigolyn gael gwybodaeth fanwl mewn perthynas â'r diben penodol y mae'n rhoi ei ganiatâd penodol ar ei gyfer.

14.10 Bydd angen i staff gadw cofnodion o bob datganiad o ganiatâd fel bod modd i'r Urdd ddangos ei fod yn cydymffurfio â gofynion caniatâd.

15. Cyfyngiadau ar drosglwyddo data

15.1 Mae cyfraith diogelu data yn gwahardd trosglwyddo data i wledydd y tu allan i'r Ardal Economaidd Ewropeaidd (AEE) er mwyn sicrhau nad yw lefel y diogelu data sy'n cael ei rhoi i unigolion yn cael ei thanseilio. Mae data personol yn cael ei drosglwyddo o'r wlad wreiddiol ar draws ffiniau pan gaiff ei drosglwyddo, ei anfon, ei weld neu ei ddefnyddio mewn gwlad wahanol.

15.2 Dim ond os yw un o'r amodau canlynol yn gymwys y gall yr Urdd drosglwyddo data personol y tu allan i'r AEE:

(a) mae'r Comisiwn Ewropeaidd wedi cyhoeddi penderfyniad yn cadarnhau bod y wlad y mae'r data personol yn cael ei drosglwyddo iddi yn sicrhau lefel ddigonol o ddiogelwch ar gyfer hawliau a rhyddid yr unigolyn ('penderfyniad digonolrwydd');

(b) mae mesurau diogelu priodol yn eu lle megis rheolau corfforaethol rhwymol (sy'n gymalau cytundebol safonol sydd wedi'u cymeradwyo gan y Comisiwn Ewropeaidd), cod ymddygiad cymeradwy neu fecanwaith ardystio;

(c) mae'r unigolyn wedi rhoi caniatâd penodol i'r trosglwyddiad arfaethedig ar ôl cael gwybod am unrhyw risgiau posibl; neu

(d) mae angen trosglwyddo ar gyfer un o'r rhesymau eraill sydd wedi'u nodi o dan y gyfraith diogelu data, gan gynnwys cyflawni contract rhwng yr Urdd a'r unigolyn, rhesymau er budd y cyhoedd, sefydlu, ymarfer neu amddiffyn hawliadau cyfreithiol neu ddiogelu buddiannau hanfodol yr unigolyn lle nad yw'r unigolyn yn gorfforol neu'n gyfreithiol yn gallu rhoi caniatâd ac, mewn rhai achosion cyfyngedig, er buddiannau cyfreithlon yr Urdd.

15.3 Dylai staff gysylltu â'r Rheolwr Preifatrwydd Data cyn trosglwyddo data personol y tu allan i'r AEE i sicrhau bod un o'r amodau sydd wedi'u hamlinellu uchod wedi'u bodloni.

16. Rhannu Data Personol

16.1 Yn gyffredinol, ni chaniateir i'r Urdd rannu data personol gyda thrydydd parti oni bai fod mesurau diogelwch arbennig a threfniadau cytundebol penodol wedi'u sefydlu. Dylid cyfeirio unrhyw gais am rannu data personol at Gyfarwyddwr yr adran berthnasol.

16.2 Dim ond os bydd gan y derbynnydd reswm sy'n ymwneud â'i swydd dros wybod yr wybodaeth, a bod y trosglwyddiad yn cydymffurfio ag unrhyw gyfyngiadau trosglwyddo ar draws ffiniau, y gall staff rannu'r data personol sy'n cael ei gadw gan yr Urdd â chyflogai arall.

16.3 Lle mae'r Urdd yn defnyddio sefydliadau allanol i brosesu data personol ar ei ran, mae angen gweithredu trefniadau diogelwch ychwanegol mewn contractau gyda'r sefydliadau hynny i sicrhau diogelwch data personol.

16.4 Dylai staff ymgynghori â'r Rheolwr Preifatrwydd Data i drafod y camau angenrheidiol i sicrhau cydymffurfio wrth sefydlu unrhyw gytundeb newydd neu newid unrhyw gytundeb presennol.

17. Hawliau a cheisiadau unigolion

17.1 Mae gan unigolion hawliau ynglŷn â'r ffordd y mae'r Urdd yn trin eu data personol. Mae'r rhain yn cynnwys hawliau i:

(a) dderbyn gwybodaeth benodol am weithgareddau prosesu'r Urdd mewn hysbysiad preifatrwydd (gweler adran 5.7uchod);

(b) gofyn am fynediad at eu data personol y mae'r Urdd yn ei gadw (trwy gais am fynediad at ddata gan y testun – 'subject access request') (mynediad);

(c) gofyn i'r Urdd ddileu data personol os nad yw bellach yn angenrheidiol mewn perthynas â'r dibenion y cafodd ei gasglu neu ei brosesu ar eu cyfer (dileu);

(d) cywiro data anghywir neu gwblhau data anghyflawn (cywiro);

(e) cyfyngu ar brosesu mewn amgylchiadau penodol (cyfyngiad);

(f) mewn amgylchiadau cyfyngedig, derbyn neu ofyn am drosglwyddo eu data personol i drydydd parti mewn fformat strwythuredig, sy'n cael ei ddefnyddio'n gyffredin ac sy'n ddarllenadwy gan beiriant (cludadwyedd data);

(g) tynnu'n ôl eu caniatâd i brosesu ar unrhyw adeg;

(h) atal defnydd yr Urdd o'u data personol at ddibenion marchnata uniongyrchol;

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

(j) gofyn am gopi o gytundeb sy'n sail i drosglwyddo data personol y tu allan i'r AEE;

(k) gwrthwynebu penderfyniadau yn seiliedig ar brosesu awtomatig yn unig (h.y. pan gaiff penderfyniad sy'n seiliedig ar brosesu awtomatig yn unig ei wneud (gan gynnwys proffilio) sy'n cynhyrchu effeithiau cyfreithiol neu'n effeithio'n sylweddol ar unigolyn);

(l) atal prosesu sy'n debygol o achosi difrod neu ofid i'r unigolyn neu unrhyw un arall;

(m) cael gwybod am achos o dorcyfraith ym maes data personol sy'n debygol o arwain at risg uchel i'w hawliau a'u rhyddid;

(n) cwyno i'r awdurdod goruchwylio.

17.2 Rhaid i staff anfon unrhyw gais sydd wedi'i dderbyn mewn perthynas â'r hawliau sydd wedi'u hamlinellu uchod i'r Rheolwr Preifatrwydd Data ar unwaith. Mae hyn yn arbennig o bwysig oherwydd mae rhaid i'r Urdd ymateb i gais dilys o fewn y terfynau amser sydd wedi'u rhagnodi yn gyfreithiol (o dan Rheoliadau Diogelu Data Cyffredinol, yn y rhan fwyaf o amgylchiadau, hyd y cyfnod hwn yw 1 mis o ddyddiad derbyn y cais).

18. Marchnata uniongyrchol

18.1 Mae'r Urdd yn ddarostyngedig i reolau penodol a chyfreithiau preifat wrth farchnata i'n haelodau, cyn-aelodau a darpar aelodau.

18.2 Mae angen caniatâd ymlaen llaw bob amser ar gyfer marchnata uniongyrchol electronig (er enghraifft, trwy e-bost, neges destun neu alwadau awtomataidd).

18.3 Rhaid cynnig yr hawl i wrthwynebu marchnata uniongyrchol (h.y. dewis peidio â derbyn gwasanaeth neu ddad-danysgrifio) i'r unigolyn mewn ffordd ddeallus fel bod modd gwahaniaethu'n glir rhwng y dewis hwn a gwybodaeth arall, pan fydd data personol yr unigolyn yn cael ei gasglu ac ym mhob cyfathrebiad dilynol.

18.4 Rhaid i wrthwynebiad unigolyn i farchnata uniongyrchol gael ei fodloni yn brydlon. Os bydd cwsmer neu aelod yn dewis peidio â derbyn gwasanaeth ar unrhyw adeg, dylid ynysu eu manylion cyn gynted ag y bo modd. Mae ynysu yn golygu cadw digon o wybodaeth i sicrhau bod dewisiadau marchnata yn cael eu parchu yn y dyfodol.

19. Adrodd am achos o Dorcyfraith yn ymwneud â Data Personol

19.1 Mae cyfraith diogelu data yn mynnu bod yr Urdd yn rhoi gwybod am achosion o dorcyfraith sy'n ymwneud â Data Personol i'r awdurdod goruchwylio perthnasol (at ein dibenion ni, Swyddfa'r Comisiynydd Gwybodaeth yw hyn fel rheol) a thestun y data unigol, dan rai amgylchiadau.

19.2 Dylai staff fod yn ymwybodol bod torcyfraith yn ymwneud â data personol yn golygu unrhyw weithred neu hepgoriad sy'n peryglu diogelwch, cyfrinachedd, uniondeb neu argaeledd data personol neu ddiogelwch corfforol, technegol, gweinyddol neu drefniadol y mae'r Urdd neu ein darparwyr gwasanaeth trydydd parti wedi'u rhoi ar waith i'w warchod. Mae colli data personol, neu ei ddatgelu neu ei gaffael heb awdurdod, yn dorcyfraith yn ymwneud â data personol.

19.3 Os yw staff yn gwybod neu'n amau bod torcyfraith yn ymwneud â data personol wedi digwydd, ni ddylent geisio ymchwilio i'r mater eu hunain. Dylai staff gysylltu ar unwaith â'r person neu'r tîm sydd wedi'u penodi fel y pwynt cyswllt allweddol ar gyfer torcyfraith yn ymwneud â data personol a'r Rheolwr Preifatrwydd Data.

19.4 Dylai staff sicrhau eu bod yn cadw'r holl dystiolaeth sy'n berthnasol i'r achos o dorcyfraith yn ymwneud â data personol ag sy'n bosib.

20. Canlyniadau methu â chydymffurfio

20.1 Mae'r cydymffurfio â'r Polisi Diogelu Data hwn yn rhywbeth y mae'r Urdd yn ei gymryd o ddifrif. Mae methu â chydymffurfio yn rhoi staff a'r Urdd mewn perygl. Mae pwysigrwydd y polisi diogelu data hwn yn golygu bod methu â

chydymffurfio ag unrhyw ofyniad yn gallu arwain at gamau disgyblu. Gallai hyn arwain at ddiswyddo.

20.2 Mae'r Urdd yn cadw'r hawl i newid y Polisi Diogelu Data hwn ar unrhyw adeg heb rybudd. Dylai staff sicrhau bod ganddynt y copi diweddaraf o'r Polisi Diogelu Data hwn.

21. ADOLYGIAD O'R POLISI

21.1 Crewyd y Polisi Diogelu Data ar y dyddiad isod ac fe'i adolygir yn flynyddol. .

22. Cydnabod derbyn ac adolygu'r polisi

22.1 Bydd y polisi hwn ar gael i bob aelod o staff a gwirfoddolwr naill ai ar-lein neu ar ffurf brintiedig. Bydd gofyn i bob gweithiwr a gwirfoddolwr gydnabod eu bod wedi derbyn a darllen copi o Bolisi Diogelu Data'r Urdd ac yn deall eu bod yn gyfrifol am wybod a glynu wrth ei delerau. Bwriedir i'r wybodaeth yn y Polisi Diogelu Data hwn helpu staff a gwirfoddolwyr i weithio gyda'i gilydd yn effeithiol wrth gyflawni cyfrifoldebau eu swyddi ac i'w cynorthwyo wrth ddefnyddio a diogelu data personol. Nid yw'r Polisi Diogelu Data hwn yn pennu telerau nac amodau cyflogaeth nac yn ffurfio rhan o gontract cyflogaeth.

Polisi Diogleu Data

Fersiwn 4

Rhagfyr 2021

Arwyddwyd

Sian Lewis

Prif Weithredwr