Polisi Asesiad o'r Effaith ar Ddiogelu Data

Cynnwys

1. Diben

1.1. Mae'r Ombwdsmon Gwasanaethau Cyhoeddus Cymru yn cymryd preifatrwydd data personol yn gwbl ddifrifol. Mae gennym fesurau ar waith i ddeall pa ddata personol sydd gennym ac i sicrhau y caiff data ei ddiogelu yn ddigonol.

1.2. Gyda chymaint o wybodaeth yn cael ei chasglu, ei defnyddio a'i rhannu, mae'n bwysig bod camau yn cael eu cymryd i ddiogelu preifatrwydd pob unigolyn a sicrhau bod gwybodaeth bersonol yn cael ei thrin yn gyfreithiol, yn ddiogel, yn effeithlon ac yn effeithiol.

1.3. Mae ein rhwymedigaethau o dan Reoliad Cyffredinol ar Ddiogelu Data'r DU (GDPR y DU) yn ei gwneud yn ofynnol i ni ystyried materion diogelu data a phreifatrwydd ymlaen llaw ar gyfer unrhyw ddata personol a broseswn. Offeryn i gyflawni hyn yw'r Asesiad o'r Effaith ar Ddiogelu Data (DPIA) ac ystyrir yn elfen allweddol o ddull 'Preifatrwydd trwy Ddylunio'. [1] Bydd cwblhau DPIA yn ein cynorthwyo i nodi a lleihau ein risgiau preifatrwydd i gydymffurfio â'n rhwymedigaethau diogelu data a chwrdd â disgwyliadau unigolion o ran preifatrwydd. Mae'r polisi hwn, y canllawiau a'r ffurflenni cysylltiedig yn nodi'r cydrannau allweddol dan sylw.

1.4. Mae'r polisi hwn yn rhan o fframwaith llywodraethu gwybodaeth Ombwdsmon Gwasanaethau Cyhoeddus Cymru (OGGC).

2. Cwmpas

2.1. Dylai'r polisi hwn fod yn berthnasol i holl staff OGCC (gan gynnwys staff parhaol, contract a dros dro ac unigolion neu sefydliadau sydd wedi'u contractio'n uniongyrchol gan OGCC).

3. Beth yw DPIA?

3.1. Proses o nodi risgiau diogelu data prosiect, proses neu system, yn systematig ac yn gynhwysfawr, yw DPIA. Yna gellir dadansoddi'r risgiau hyn i leihau neu fynd i'r afael â'r risg.

[1] Canllawiau DPIA Swyddfa'r Comisiynydd Gwybodaeth (ICO)

3.2. Gall y risgiau hyn fod yn risgiau cyfreithlon, ariannol, yn ymwneud ag enw da neu'n risgiau cydymffurfio, ond dylai'r ffocws fod ar y risgiau i unigolion, megis y potensial ar gyfer unrhyw anfantais neu niwed sylweddol. Rhaid i'r DPIA ystyried tebygolrwydd a difrifoldeb unrhyw effaith ar unigolion. Nid oes rhaid dileu'r risg ond rhaid ei ostwng i lefel y mae OGCC yn ei dderbyn.

3.3. Mae'n rhwymedigaeth o dan GDPR y DU i gynnal DPIA ar gyfer unrhyw brosesu sy'n debygol o arwain at risg uchel i fuddiannau unigolion. Ar ôl cynnal DPIA, os yw'r risg yn parhau'n uchel ac nad oes modd lliniaru'r risg, yna rhaid ymgynghori â Swyddfa'r Comisiynydd Gwybodaeth (ICO) cyn dechrau'r prosesu.

3.4. Dylid ymgorffori DPIA ym mhrosesau sefydliadol. Mae gan OGCC Gofrestr Asedau Gwybodaeth sy'n rhestru'r asedau gwybodaeth sydd gennym, a chaiff y rhain eu grwpio yn ôl swyddogaeth busnes. Dylid cysylltu DPIA ag ased gwybodaeth a'i gofnodi yn y Gofrestr Asedau Gwybodaeth. Ni ddylai DPIA fod yn asesiad unwaith ac am byth ond yn un sy'n cael ei adolygu'n rheolaidd.

4. Diffiniadau eraill

4.1. **Menter** - unrhyw gynnig sy'n ystyried newid, er enghraifft polisi, proses, gweithdrefn, prosiect, system TG neu weithgarwch caffael newydd.

4.2. **Preifatrwydd** – yn ei ystyr ehangaf, hawl unigolyn i fod yn rhydd rhag ymyrraeth.

4.3. **Ased Gwybodaeth** – corff o wybodaeth sydd wedi'i ddiffinio a'i reoli fel un uned unigol er mwyn gallu ei ddeall, rhannu, diogelu a'i ddefnyddio'n effeithlon. Mae ganddynt werth, risg, cynnwys a chylch oes sy'n adnabyddadwy a hylaw.[2]

4.4. **Y Gofrestr Asedau Gwybodaeth** - rhestr o asedau gwybodaeth sydd gan OGCC. Mae'r gofrestr yn ein galluogi i ddeall a rheoli risgiau sy'n gysylltiedig â phob ased gwybodaeth.

4.5. **Data personol** – gwybodaeth sy'n ein galluogi i nodi unigolyn, naill ai o'r wybodaeth a ddarparwyd neu o'i hychwanegu at wybodaeth

[2] Taflen Ffeithiau Ased Gwybodaeth, Yr Archifau Cenedlaethol

arall a allai fod ar gael. Gallai data personol hefyd gynnwys categorïau arbennig o ddata personol sy'n cael eu hystyried yn fwy sensitif y bydd ond yn bosibl eu prosesu mewn amgylchiadau mwy cyfyngedig.

5. Rolau a chyfrifoldebau

Rôl	Cyfrifoldeb Llywodraethu Gwybodaeth (IG)
Bob Aelod o Staff	Mae angen i unrhyw aelod o staff sy'n ymwneud â datblygu prosiect, menter a systemau fod yn ymwybodol o'r polisi hwn a deall pryd y gallai fod angen DPIA. Dylent adolygu'r DPIA trwy gydol y prosiect ac ymgynghori â'r IGM.
Perchnogion Asedau Gwybodaeth (IAO)	IAO yw unigolion cyfrifol/unigolion mewn swyddi uchel sy'n gweithio mewn maes busnes perthnasol. Mae angen iddynt ddeall a mynd i'r afael â risgiau i asedau gwybodaeth y maent yn 'berchen' arnynt trwy ddeall pa wybodaeth sy'n cael ei phrosesu yn eu maes busnes, sut a pham. Mae'n rhaid iddynt roi sicrwydd i'r SIRO (yr Uwch Berchennog Risgiau Gwybodaeth) ar ddiogelwch a defnydd asedau gwybodaeth a bod DPIA yn cael eu cynnal ar gyfer unrhyw brosiectau, systemau a phrosesau newydd.
Cynorthwywyr Asedau Gwybodaeth (IAA)	Mae IAA yn cynorthwyo IAO wrth sicrhau bod polisïau a phrosesau yn cael eu dilyn, gan gydnabod risgiau diogelwch gwybodaeth gwirioneddol neu bosibl. Maent yn sicrhau bod y gofrestr ased gwybodaeth yn cael ei diweddaru ac yn cynorthwyo'r IAO i gwblhau DPIA.
Cynorthwywyr Asedau Gwybodaeth (IAA)	Mae IAA yn cynorthwyo IAO gan sicrhau bod polisïau a phrosesau yn cael eu dilyn, drwy gydnabod risgiau diogelwch gwybodaeth gwirioneddol neu bosibl. Maent yn sicrhau bod y gofrestr ased gwybodaeth yn cael ei diweddaru ac yn cynorthwyo'r IAO i gwblhau DPIA.
Y Grŵp Diogelwch Gwybodaeth (ISG)	Yr ISG yw'r grŵp llywio sy'n goruchwylio cydymffurfiaeth â llywodraethu gwybodaeth, safonau diogelwch a'r polisi hwn. Mae'r grŵp yn gyfrifol am gymeradwyo Fframwaith Strategol Llywodraethu Gwybodaeth OGCC a chynlluniau gweithredu blynyddol sy'n cynnwys adolygu asedau gwybodaeth a nodir yng Nghofrestr Asedau Gwybodaeth OGCC.

Rôl	***Cyfrifoldeb Llywodraethu Gwybodaeth (IG)***
Rheolwr Llywodraethu Gwybodaeth (IGM)	Yr IGM yw Swyddog Diogelu Data (DPO) statudol y sefydliad ac mae'n gyfrifol am fonitro cydymffurfiad sefydliadol â deddfwriaeth diogelu data gan gynnwys y polisi hwn. Maent yn gyfrifol am weithredu'r polisi hwn a rhaid ymgynghori â nhw o ran unrhyw DPIAau a gynhelir.
Y Prif Swyddog Diogelwch Gwybodaeth (CISO)	Y COODol yw'r CISO a'i rôl yw sicrhau diogelwch gwybodaeth OGCC, gan gynnwys seiberddiogelwch a chadernid rhwydweithiau OGCC. Maent yn gweithio â'r SIRO a DIPO i gynghori ynghylch y ffordd orau i reoli risg, tra'n manteisio ar dechnoleg i gyflawni amcanion strategol y sefydliad. Mae'r SIRO a CISO yn gyfrifol am gymeradwyo DPIA.
Yr Uwch Berchennog Risgiau Gwybodaeth (SIRO)	Y CLADol yw'r SIRO a'i rôl yw arwain diwylliant o reoli gwybodaeth yn dda. Maent yn gyfrifol am sicrhau bod risgiau gwybodaeth sydd eisoes wedi'u nodi yn cael eu rheoli a bod cynlluniau rheoli yn cael eu gweithredu. Mae'r SIRO a CISO yn gyfrifol am gymeradwyo DPIA.

6. Er Buddion Asesiad o'r Effaith ar Ddiogelu Data

6.1. nad yw cwblhau Asesiad o'r Effaith ar Ddiogelu Data (DPIA) yn ofyniad cyfreithlon, mae'n ffordd effeithiol o ddangos sut mae'r dulliau prosesu data personol yn cydymffurfio â deddfwriaeth diogelu data. Gallai'r ICO holi a yw DPIA wedi'i gynnal.

6.2. Mae DPIA yn sicrhau bod y dewisiadau lleiaf ymwthiol i breifatrwydd yn cael eu harchwilio er mwyn atal rhag effeithio unigolion mewn ffordd negyddol. Mae'n helpu i nodi pa wybodaeth sydd angen ei chynnwys mewn hysbysiad preifatrwydd, sy'n cynorthwyo â thryloywder, gan ei gwneud hi'n haws esbonio i unigolion pam mae eu gwybodaeth yn cael ei defnyddio. Dylai hyn arwain at fwy o hyder yn y ffordd y caiff gwybodaeth bersonol ei phrosesu.

6.3. Bydd cwblhau DPIA yn ystod camau cynnar menter yn sicrhau bod materion preifatrwydd yn cael eu nodi'n gynnar. Yn bwysicach oll, nid yw datrysiadau amhriodol yn cael eu gweithredu y bydd angen eu gwrthdroi yn ddiweddarach, a allai fod yn gostus.

6.4. Dylai cynnal DPIA fod o fudd i OGCC drwy lunio polisïau a systemau gwell a gwella perthnasoedd ag unigolion.

7. Y Weithdrefn DPIA

7.1. Mae'r weithdrefn DPIA yn cynnwys 8 cam.

- Nodi'r angen am DPIA.
- Disgrifio llifoedd prosesu a gwybodaeth.
- Ystyried ymgynghori.
- Nodi ac asesu risgiau.
- Nodi mesurau lliniaru.
- Cymeradwyo a chofnodi canlyniadau.
- Integreiddio'r canlyniadau mewn cynllun.
- Adolygu'n rheolaidd.

7.2. Dylid graddio'r amser a'r adnoddau a neilltuir ar gyfer DPIA i gyd-fynd â natur y fenter.

8. Pryd y mae angen DPIA?

8.1. Gallai fod angen DPIA ar gyfer unrhyw fenter sy'n ymwneud â phrosesu data personol. Dylid ymgymryd â DPIA o ddechrau'r fenter newydd er mwyn sicrhau bod problemau posibl yn cael eu nodi'n gynnar, pan fydd mynd i'r afael â nhw yn symlach, yn llai costus a gellir dylanwadu ar gyfeiriad y gwaith. Dylid parhau i ystyried y DPIA drwy gydol y broses weithredu.

8.2. Yn ogystal, mae'n bwysig ystyried DPIA ar gyfer unrhyw newid arfaethedig i fenter bresennol. Mae newid i unrhyw broses neu system bresennol hefyd yn cynnwys terfynu unrhyw weithgaredd neu drefniant. Er enghraifft, pam ddaw contract i ben, fel y gellir ystyried trefniadau ar gyfer dinistrio neu drosglwyddo unrhyw ddata yn ddiogel. O ran gweithgareddau caffael, dylid cwblhau'r DPIA cyn tendro er

mwyn sicrhau bod yr holl risgiau preifatrwydd perthnasol yn cael eu hystyried wrth baratoi manylebau tendro.

8.3. Mae DPIA yn ofynnol cyn dechrau unrhyw brosesu sy'n 'risg uchel'. Mae'r weithdrefn DPIA yn dechrau gyda gwirio a yw'r fenter yn cynnwys unrhyw brosesu sy'n gofyn yn awtomatig am DPIA neu ffactorau eraill a allai ddangos bod y risg yn debygol o fod yn uchel. Er enghraifft, defnyddio cyflenwr allanol i brosesu data personol.

8.4. Os mai canlyniad y sgrinio yw nad oes angen DPIA, dylid dogfennu'r rheswm am hyn. Gall fod angen adolygu'r penderfyniad yn y dyfodol. Hyd yn oed os nad oes angen DPIA, efallai y bydd yr offer mapio llif ac asesu risg o fudd i chi ar gyfer rheoli prosiect.

9. Ymgymryd â DPIA

9.1. Ar ôl dod i gasgliad bod angen DPIA llawn, dylid cwblhau'r Templed DPIA. Mae'r templed yn egluro beth sy'n ofynnol ym mhob cam. Mae'n rhaid rhoi esboniad am unrhyw adran sydd heb ei chwblhau.

9.2. Cyfrifoldeb arweinydd menter yw nodi'r angen am DPIA a'i gwblhau.

9.3. **Disgrifio llifoedd prosesu a gwybodaeth.** Mae'r cam hwn yn ymwneud â disgrifio natur, cwmpas, cyd-destun a diben y prosesu:

- **Natur** - Sut bydd y data'n cael ei gasglu, ei ddefnyddio, ei storio, ei ddileu a'i rannu?
- **Cwmpas** - Y math o ddata dan sylw ac a yw hyn yn cynnwys data categori arbennig neu ddata euogfarn droseddol? Faint o ddata fydd yn cael ei gasglu a'i ddefnyddio a pha mor hir y bydd yn cael ei gadw? Nifer y bobl yr effeithir arnynt.
- **Cyd-destun** - Perthynas OGCC â'r unigolion. Faint o reolaeth fydd ganddynt ac a fyddent yn disgwyl i ni ddefnyddio eu data fel y cynigir? A ydynt yn cynnwys plant neu unrhyw grwpiau eraill sy'n agored i niwed?
- **Diben** - Pam y mae OGCC yn prosesu'r data? Beth yw'r effaith a fwriedir ar unigolion? Beth yw'r manteision i OGCC?

9.4. Gall defnyddio diagram llif fod yn defnyddio i fapio'r llif gwybodaeth o ddechrau'r broses hyd at ddiwedd y prosesu. Mae hyn yn caniatáu ar gyfer asesiad effeithiol o risgiau preifatrwydd trwy gylch oes y prosesu.

9.5. **Ystyriwch ymgynghori** i ddeall a yw'r prosesu yn angenrheidiol ac yn gymesur. Dylech ystyried ceisio barn unigolion neu eu cynrychiolwyr a allai gael eu heffeithio gan y prosesu. Mae'n bwysig ystyried ymgynghori â rhanddeiliad mewnol ac allanol ac unrhyw un sy'n gyfrifol am unrhyw ran o'r prosesu. Gall fod angen cael cyngor arbenigol, megis arbenigedd cyfreithiol a diogelwch gwybodaeth.

Nid oes unrhyw ofyniad penodol i ymgynghori ond gall helpu i nodi ac asesu'r risgiau diogelu data ac unrhyw risgiau eraill.

9.6. **Nodi ac asesu risgiau** trwy gylch oes y prosesu. Er enghraifft, risgiau ynghylch cywirdeb neu ddiogelwch y data personol ac unrhyw ymyrraeth ddiangen ar hawl unigolion i breifatrwydd. Hefyd, gall fod risgiau i'r sefydliad megis risgiau cydymffurfio cyfreithiol, risgiau ariannol neu risgiau i enw da.

9.7. **Nodi mesurau lliniaru** i leihau neu ddileu'r risg, gan ystyried unrhyw gostau a buddion, ynghyd ag a allai'r rhain fod yn briodol. Er enghraifft:

- Penderfynu peidio â chasglu mathau penodol o ddata.
- Dienwi neu ffugenwi'r data lle bo modd.
- Datblygu canllawiau neu brosesau i osgoi risgiau.
- Hyfforddi staff.
- Defnyddio technoleg wahanol neu ychwanegu lefelau ychwanegol o ddiogelwch.
- Newid hysbysiadau preifatrwydd fel bod unigolion yn gwybod beth i'w ddisgwyl.

9.8. **Cymeradwyo a chofnodi canlyniadau** o'r asesiad risg. Efallai na fydd yn bosibl dileu neu leihau'r risg felly mae angen cofnodi hyn. Gall rhai risgiau, gan gynnwys risg uchel, gael eu hystyried yn dderbyniol ar sail y manteision i OGCC. Fodd bynnag, rhaid ymgynghori â'r ICO os yw'r risg yn parhau i fod yn uchel ac efallai y bydd yn anodd ei liniaru.

Gallai hefyd fod yn angenrheidiol diweddaru Cofrestr Risgiau OGCC. Mae'n rhaid i'r Templed DPIA gael ei arwyddo gan y Perchennog Asedau Gwybodaeth (IAO). Dylid dogfennu cyngor yr IGM ac os ydych yn penderfynu peidio â dilyn eu cyngor, rhaid cofnodi'r rhesymau dros hyn hefyd.

9.9. **Integreiddio canlyniadau yn y cynllun** er mwyn nodi camau gweithredu clir a pherchnogion camau gweithredu clir. Bydd angen monitro cynlluniau gweithredu hyd at eu gweithredu. Mae'n bosibl y gallai hyn fwydo yn uniongyrchol i'r ddogfennaeth rheoli prosiect. Gallai fod yn angenrheidiol fynd drwy'r cylch DPIA eto ac addasu'r cynllun gweithredu.

10. Ymgynghori â'r ICO

10.1. Mae'n rhaid ymgynghori â'r ICO cyn bwrw ymlaen â'r prosesu pan fydd y risg sy'n anodd cael gwared arno yn un uchel, ac nad yw'n bosibl lleihau neu ddileu'r risg.

10.2. Ni ellir bwrw ymlaen â'r prosesu hyd nes yr ymgynghorwyd â'r ICO a gall gymryd rhwng 8 a 14 wythnos i'r ICO ymateb.

10.3. Bydd yr IGM yn cysylltu â'r ICO i anfon copi o'r DPIA.

11. Adolygu DIPA

11.1. Dylid adolygu'r DPIA a'i ailadrodd os bydd newid sylweddol i natur, cwmpas, cyd-destun neu ddibenion y prosesu.

12. Datgelu a chyhoeddi DPIA

12.1. Er nad yw datgelu neu gyhoeddi DPIA wedi'i gwblhau yn ofyniad cyfreithiol, mae datgelu neu gyhoeddi yn dangos atebolrwydd a thryloywder. Gall ennill ymddiriedaeth a hyder ym mhrosesau prosesu gwybodaeth bersonol OGCC.

12.2. Gellir gofyn am fynediad i DPIA o dan Ddeddf Rhyddid Gwybodaeth 2000. Felly, oni bai bod eithriad yn berthnasol, efallai y bydd angen ei ddatgelu.

12.3. Bydd angen ystyried cyhoeddi ar sail pob achos unigol, gan sicrhau na chaiff unrhyw wybodaeth sensitif ei datgelu. Y Perchennog Asedau Gwybodaeth, ynghyd â'r Rheolwr Llywodraethu Gwybodaeth, SIRO a CISO, ddylai benderfynu a ddylid cyhoeddi.

12.4. Dylid ymgynghori â'r IGM cyn gwneud unrhyw benderfyniadau o ran datgelu neu gyhoeddi DPIA.

13. Monitro a Chydymffurfio

13.1. Bydd y Rheolwr Llywodraethu Gwybodaeth yn monitro effeithiolrwydd y polisi hwn, gan ddarparu adroddiadau yn ôl yr angen i'r ISG a'r Tîm Rheoli.

13.2. Fel egwyddor o arfer da, ac i sicrhau bod Cofrestr Asedau Gwybodaeth OGCC yn cael ei diweddaru'n gyson, gellir adolygu DPIA ac asesiadau risg eraill pryd bynnag y caiff ased gwybodaeth ei adolygu.

13.3. Mae'r IGM ar y cyd a'r IAO ac ISG yn adolygu tueddiadau digwyddiadau diogelwch gwybodaeth i sicrhau bod rheolaethau digonol ar waith sy'n briodol i unrhyw risgiau diogelu data. O ganlyniad, gellir adolygu adolygiadau o unrhyw DPIA perthnasol.

14. Adolygu'r polisi hwn

14.1. Caiff y polisi hwn ei adolygu pob 3 mlynedd a chaiff ei gyhoeddi'n fewnol ac yn allanol.

15. Rhagor o Wybodaeth

15.1. Mae Canllawiau Proses DPIA OGCC yn cefnogi'r staff hynny sy'n ymgymryd â DPIA ac yn darparu cyfarwyddiadau cam wrth gam ynglŷn â'r hyn sy'n ofynnol drwy gydol y broses. Mae copi o holiadur sgrinio DPIA a Ffurflen Templed DPIA wedi'u cynnwys yn ogystal ag enghraifft o DPIA wedi'i gwblhau.

15.2. Gall y Rheolwr Llywodraethu Gwybodaeth (IGM) roi cyngor ac arweiniad a rhaid ymgynghori â'r IGM yn ystod y broses DPIA.

15.3. Adnoddau allanol:

- Asesiadau o'r Effaith ar Ddiogelu Data, Canllawiau ICO.
- Canllawiau DPIA manwl gan ICO.