
Polisi a Gweithdrefn Rheoli Digwyddiad Diogelwch Gwybodaeth

Cynnwys

1.	Cyflwyniad a diffiniadau	3
2.	Mathau o ddigwyddiadau	4
3.	Ystyried risgiau	4
4.	Y weithdrefn	5
5.	Cyfyngu ac adfer (cam 1).....	6
6.	Asesu'r risg (cam 2)	7
7.	Hysbysiad o'r achos o dor diogelwch (cam 3).....	8
8.	Gwerthuso ac ymateb (cam 4).....	9
9.	Monitro ac adolygu	10
10.	Atodiad un: siart llif o'r gofynion hysbysu.....	11

1. Cyflwyniad a diffiniadau

- 1.1 Mae Ombwdsmon Gwasanaethau Cyhoeddus Cymru (Yr Ombwdsmon) yn cadw swm mawr o ddata personol a gwybodaeth categorïau arbennig. Mae'n rhaid i bob aelod o staff gymryd pob gofal i ddiogelu'r wybodaeth hon. Os bydd data yn cael ei golli neu'n cael ei rannu'n amhriodol, mae'n rhaid i ni gymryd camau priodol i leihau unrhyw risgiau cysylltiedig.
- 1.2 Cyfeirir at golli neu rannu data yn amhriodol, yn wirioneddol neu'n amheus yn y ddogfen fel 'digwyddiad diogelwch gwybodaeth'
- 1.3 Mae'r ddogfen hon yn cyflwyno gweithdrefn yr Ombwdsmon ar gyfer ystyried digwyddiadau sy'n arwain at dor diogelwch data personol Deddf Diogelu Data 2018 (DPA) neu'r Rheoliad Cyffredinol ar Ddiogelu Data (GDPR) a chyfreithiau cysylltiedig. Mae'r broses yn seiliedig ar ganllawiau'r ICO¹ a chanllawiau a gyhoeddwyd gan Weithgor Diogelu Data Erthygl 29².
- 1.4 Gall digwyddiad diogelwch gwybodaeth effeithio ar gyfrinachedd, integreidd neu argaeledd data. Mae'n rhaid asesu digwyddiad yn gyflym i sefydlu a fu achos o dor diogelwch data personol.
- 1.5 Diffinnir tor diogelwch data personol fel:

...tor diogelwch sy'n arwain at ddinistrio, colli, addasu, datgeliad anawdurdodedig, neu fynediad at, ddata personol. Mae hyn yn cynnwys tor diogelwch o ganlyniad i achosion damweiniol a bwriadol. Mae hefyd yn golygu bod y tor diogelwch yn fwy na cholli data personol yn unig.¹

¹ [Canllawiau'r ICO ar dor diogelwch data personol](#)

² Gweithgor Erthygl 29: [Canllawiau ar hysbysu achosion o dor diogelwch data personol o dan Reoliad 2016/679](#) (Diwygiwyd a Mabwysiadwyd 6 Chwef 2018)

- 1.6 Gall asesiad ddod i'r casgliad nad oedd yn achos o dor diogelwch data personol. Fodd bynnag, mae'r asesiad yn darparu cyfle i adolygu mesurau sefydliadol a thechnegol er mwyn lliniaru risgiau posibl yn y dyfodol.

2. Mathau o ddigwyddiadau

- 2.1 Gall enghreifftiau o ddigwyddiadau gynnwys:
- Mynediad gan drydydd parti anawdurdodedig
 - Gweithred (neu ddiffyg gweithredu) bwriadol neu ddamweiniol
 - Anfon data personol at dderbynydd anghywir neu heb awdurdod priodol
 - Dyfeisiau sy'n cynnwys data personol yn cael eu colli neu eu dwyn
 - Addasu data personol heb ganiatâd, a
 - Colli argaeledd data personol, er enghraifft, am ei fod wedi'i amgryptio gan feddalwedd wystlo, neu ddata sydd wedi'i golli neu ei ddinistrio'n ddamweiniol.

3. Ystyried risgiau

- 3.1 Mae yna risgiau unigol a sefydliadol y mae angen eu hystyried wrth ymchwilio i ddigwyddiad. Gallai cyfaddawdu cyfrinachedd gwybodaeth, integredd neu argaeledd data arwain at:
- niwed i enw da,
 - effaith niweidiol ar ddarparu gwasanaeth,
 - niwed i unigolyn/unigolion,
 - diffyg cydymffurfiaeth ddeddfwriaethol, a/neu
 - costau ariannol.
- 3.2 Wrth ystyried y canlyniadau negyddol posibl i unigolion mae Datganiad 85 GDPR yn esbonio:

Gall tor diogelwch data personol, os nad eir i'r afael ag ef mewn dull priodol ac amserol, arwain at niwed corfforol, perthnasol ac amherthnasol i'r [unigolyn]...

- 3.3 Mae Datganiad GDPR yn darparu rhestr o ganlyniadau posibl i'r unigolyn:
- colli rheolaeth dros eu data personol;
 - cyfyngiadau i'w hawliau;
 - gwahaniaethu;
 - dwyn neu dwyll hunaniaeth;
 - colled ariannol;
 - gwyrddroi gwybodaeth yn amhriodol a oedd o dan ffugenw;
 - niwed i enw da;
 - colli cyfrinachedd neu
 - unrhyw anfantais economaidd neu gymdeithasol arwyddocaol arall.
- 3.4 Mae'r Weithdrefn yn ceisio lliniaru'r risgiau hyn drwy sicrhau:
- bod pob aelod o staff, contractwyr a defnyddwyr trydydd parti yn ymwybodol o'r weithdrefn ar gyfer adrodd digwyddiadau a'u cyfrifoldeb i adrodd yn brydlon unrhyw ddigwyddiad maent wedi'i weld neu maent yn ei amau, neu bryder ynglŷn â diogelwch gwybodaeth;
 - yr eir i'r afael ag unrhyw ddigwyddiadau neu bryderon a adroddir, a hynny'n unol â'r weithdrefn hon;
 - yn dilyn adferiad o'r digwyddiad, bod rheolaethau presennol yn cael eu harchwilio er mwyn penderfynu ar eu digonolrwydd, a bod camau cywirol yn cael eu cymryd er mwyn lleihau'r risg y bydd digwyddiadau tebyg yn digwydd; a bod
 - systemau ar waith i alluogi i'r mathau, symiau a chostau digwyddiadau diogelwch gwybodaeth cael eu mesur, eu monitro a'u hadrodd.

4. Y weithdrefn

- 4.1 Mae gweithdrefn yr Ombwdsmon ar gyfer asesu digwyddiadau diogelwch gwybodaeth yn cael ei rhannu i'r pedwar cam canlynol:
- i) Cyfyngu ac adfer;
 - ii) Asesu'r risg;
 - iii) Hysbysu;
 - iv) Gwerthuso ac ymateb

- 4.2 Dylid cwblhau Ffurflen Asesu ac Ymateb i ddigwyddiad er mwyn dangos y camau a gymerwyd.
- 4.3 Mae'r grŵp o bobl sy'n gyfrifol am ymateb i ddigwyddiadau sydd wedi'u hadrodd yn cynnwys:

<ul style="list-style-type: none">• y Prif Swyddog Gweithredol a'r Cyfarwyddwr Gwelliannau (COODOI)
<ul style="list-style-type: none">• Prif Gyngorydd Cyfreithiol a'r Cyfarwyddwr Ymchwiliadau (CLADOI) sef yr Uwch Berchennog Risgiau Gwybodaeth (SIRO) hefyd
<ul style="list-style-type: none">• y Rheolwr TG
<ul style="list-style-type: none">• Rheolwr perthnasol ar gyfer y gwasanaeth
<ul style="list-style-type: none">• y Rheolwr Llywodraethu Gwybodaeth

- 4.4 Dylid adrodd unrhyw ddigwyddiad i'r Rheolwr TG ac aelod o'r Tîm Rheoli cyn gynted ag y daw i'r amlwg. Gellir hysbysu'r Rheolwr TG ynglŷn ag unrhyw faterion seiberddiogelwch.
- 4.5 Dylai'r Rheolwr Llywodraethu Gwybodaeth a / neu'r Rheolwr perthnasol hysbysu'r COODOI a'r CLADOI cyn gynted â phosibl er mwyn sicrhau eu bod yn ymwybodol o'r mater.
- 4.6 Bydd y Rheolwr Llywodraethu Gwybodaeth yn cofnodi'r mater yn ganolog, a bydd yn monitro cynnydd i reoli ac ymchwilio i'r digwyddiad.
- 4.7 Mae'r Ffurflen Asesu ac Ymateb ar gael o dudalennau'r Ddesg Gymorth Llywodraethu Gwybodaeth ar YR HWB.

5. Cyfyngu ac adfer (cam 1)

- 5.1 Dylai'r Rheolwr Llywodraethu Gwybodaeth ac aelodau o'r Tîm Rheoli gymryd camau ar unwaith i gyfyngu'r digwyddiad, yn seiliedig ar natur y tor diogelwch. Dylid cofnodi unrhyw gamau gweithredu yn adran 1 y Ffurflen Asesu ac Ymateb.
- 5.2 Darperir enghraifft o gamau a gymerwyd i adfer / cyfyngu'r digwyddiad isod.

Os bydd y digwyddiad yn ymwneud â phost wedi'i gamgyfeirio, dylid cysylltu â'r derbynnydd i drefnu i'w adfer:

- Os bydd yn electronig, dylid gofyn i'r derbynnydd gadarnhau bod y neges wedi'i dileu'n barhaol (gan gynnwys o'u ffolder e-bost Eitemau wedi'u Dileu);
- Os drwy'r post, dylid gwneud trefniadau i'r deunydd gael ei ddychwelyd i'r swyddfa hon (yr Ombwdsmon i ddarparu amlen ddychwelyd) neu i aelod o staff ei gasglu os yw'n lleol neu drwy negesydd [bydd yr union ddull hwn yn ddibynnol ar natur y digwyddiad a'r deunydd dan sylw];

- 5.3 Pan fydd y digwyddiad yn ymwneud â gwefan yr Ombwdsmon, dylai'r Rheolwr Llywodraethu Gwybodaeth a'r Rheolwr TG ystyried a oes angen hysbysu darparwyr y wefan a'r Tîm Polisi a Chyfathrebu. Bydd angen diwygio neu ddileu gwybodaeth ar unwaith, yn ôl yr angen.
- 5.4 Pan fydd y digwyddiad yn ymwneud â systemau neu gronfeydd data mewnol yr Ombwdsmon, dylai'r Rheolwr Llywodraethu Gwybodaeth a'r Rheolwr TG ystyried hefyd a oes angen hysbysu darparwyr cymorth a systemau TG.

6. Asesu'r risg (cam 2)

- 6.1 Ar ôl cyfyngu/adfer, dylai'r Rheolwr Llywodraethu Gwybodaeth a'r Rheolwr perthnasol gynnal asesiad o'r risg sy'n gysylltiedig â'r digwyddiad, gan ddefnyddio'r Ffurflen Asesu ac Ymateb.
- 6.2 Bydd y Ffurflen Asesu ac Ymateb yn ystyried y canlyniadau niweidiol posibl i unigolion, yn seiliedig ar ddifrifoldeb a pha mor debygol y maent o ddigwydd. Bydd y ffactorau canlynol yn cael eu hasesu:
- math o dor diogelwch (h.y. cyfrinachedd, integreidd, argaeledd)
 - math, sensitifrwydd a'r swm o ddata;
 - nifer yr unigolion sydd wedi'u heffeithio;
 - diogelwch data;
 - rhwyddineb adnabod;

- difrifoldeb y canlyniadau / niwed posibl a allai ddigwydd, gan gynnwys:
 - colled ariannol;
 - gofid;
 - enw da;
 - dwyn hunaniaeth;
 - gwahaniaethu;
 - colli cyfrinachedd;
 - gwyrddroi ffugenw yn ddiawdurdod;
- unrhyw rinweddau arbennig sydd gan yr yr unigolyn/unigolion a
- difrifoldeb y canlyniadau i'r Ombwdsmon.

6.3 Dywed [Gweithgor Erthygl 29](#):

Mae'r risg hon yn bodoli pan allai tor diogelwch arwain at niwed corfforol, perthnasol neu amherthnasol i'r unigolion y torrwyd diogelwch eu data.²

- 6.4 Mae angen ystyried achosion ar sail achosion unigol, gan ystyried gofid emosiynol posibl, a niwed corfforol a pherthnasol. Bydd rhai digwyddiadau neu dor diogelwch ond yn debygol o achosi anghyfleustra posibl i staff yr Ombwdsmon. Efallai y bydd eraill yn cael effaith sylweddol ar yr unigolyn y mae eu data wedi'i gyfaddawdu.
- 6.5 Ar ôl cynnal asesiad cychwynnol dylid trafod y broses barhaus o reoli'r digwyddiad gyda'r COODOI a'r CLADOI.

7. Hysbysiad o'r achos o dor diogelwch (cam 3)

- 7.1 Bydd trafodaethau gyda'r COODOI a'r CLADOI yn penderfynu'r camau i'w cymryd yng nghanau 3 a 4 (Hysbysu a Gwerthuso).
- 7.2 Mae Cam 3 yn cynnwys penderfynu pwy ddylid eu hysbysu ynghylch yr achos o dor diogelwch, yn seiliedig ar yr asesiad o risg.

- 7.3 Mae Erthygl 33 GDPR yn ei gwneud yn ofodol i hysbysu'r ICO ynglŷn â thor diogelwch oni bai y bydd yn annhebygol y byddai'r tor diogelwch yn arwain at risg i hawliau a rhyddid unigolion. Mae'n bwysig cofnodi'r rhesymeg sy'n sail i'r penderfyniad hwn.
- 7.4 Os bydd yr Asesiad Risg yn canfod ei bod yn debygol iawn neu'n debygol y bydd yr unigolion mewn risg, dylid hysbysu'r ICO heb oedi gormodol. Pan fo'n ymarferol, o fewn 72 awr o fod yn ymwybodol o'r digwyddiad.
- 7.5 Os bydd yr asesiad yn dod i'r casgliad bod y risg yn niwtral a bod data personol dan sylw, mae ffurflen hunan-asesu'r ICO yn awgrymu galwad ffôn iddynt i drafod y digwyddiad. Byddant yn cynnig cyngor ar reoli'r risg a lliniaru ei heffaith. Os bydd angen, byddant yn cymryd manylion y tor diogelwch dros y ffôn.
- 7.6 Mae Erthygl 34 hefyd yn ei gwneud yn ofynnol i unigolion gael eu hysbysu ynghylch unrhyw dor diogelwch sy'n debygol o greu risg uchel i'w hawliau a'u rhyddid, a hynny heb oedi gormodol.
- 7.7 Os gwneir penderfyniad i hysbysu'r ICO, dylai'r Ombwdsmon ddefnyddio Ffurflen Hysbysiad o Dor Diogelwch yr ICO. Mae Siart Llif Hysbysu Gweithgor Erthygl 29 ar gael hefyd ar ddiwedd y ddogfen hon, yn ogystal â'r matrices risg.

8. Gwerthuso ac ymateb (cam 4)

- 8.1 Mae Adran 4 y Ffurflen Asesu ac Ymateb yn nodi unrhyw gamau gweithredu i'w dilyn yn dilyn y digwyddiad - er enghraifft, newidiadau i bolisiâu neu ddatblygiadau i systemau TG. Pan fo'n bosibl, dylid aseinio'r camau gweithredu hyn hefyd i aelod o staff eu cwblhau.
- 8.2 Y rheolwr llinell fydd yn ystyried unrhyw gamau gweithredu angenrheidiol (anffurfiol neu ffurfiol) mewn cysylltiad ag aelod o staff a allai fod wedi bod yn gysylltiedig â'r digwyddiad. Pan fydd angen, bydd angen iddynt ystyried unrhyw bolisiâu priodol, gan gynnwys y Polisi Rheoli Perfformiad a'r Polisi Disgyblu.

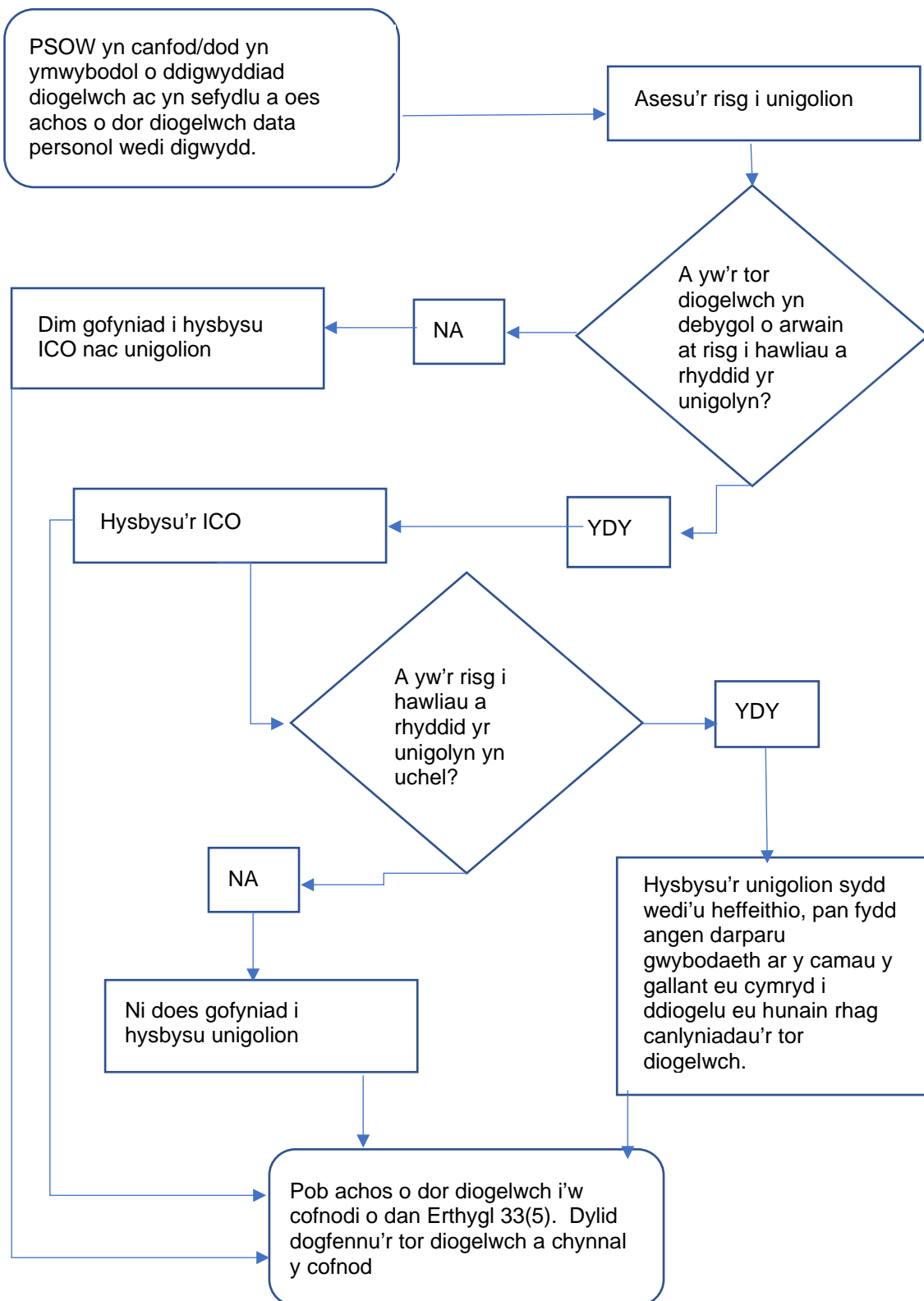
Fodd bynnag, **ni** ddylid rhestru unrhyw gamau gweithredu angenrheidiol ar y ffurflen, y gellir ei datgelu i Swyddfa'r Comisiynydd Gwybodaeth mewn achos o hysbysiad am y tor diogelwch.

- 8.3 Bydd y Rheolwr Llywodraethu Gwybodaeth yn diweddarau'r Gofrestr Digwyddiadau.

9. Monitro ac adolygu

- 9.1 Mae adroddiadau monitro Llywodraethu Gwybodaeth misol i'r Tîm Rheoli yn darparu crynodeb o ddigwyddiadau, tor diogelwch ac unrhyw gamau lliniaru angenrheidiol.
- 9.2 Mae digwyddiadau ac achosion o dor diogelwch yn cael eu hadrodd hefyd ar sail chwarterol i ARAC.
- 9.3 Bydd y Polisi a'r Weithdrefn hyn yn cael eu hadolygu bob dwy flynedd.

10. Atodiad un: Siart Ilif o'r gofynion hysbysu³



³ Yn seiliedig ar siart Ilif Gweithgor Erthygl 29 yn y Canllawiau A29WP (gweler troednodyn 2).