**Y WEITHREFN TORIADAU diogelWCH DATA AR GYFER STAFF**

**Cyflwyniad**

Mae’r Brifysgol yn dal data personol miloedd o staff, ymgeiswyr, myfyrwyr, cynfyfyrwyr, ymchwilwyr ac eraill y mae ganddynt gysylltiad â’r Brifysgol.

Gall toriadau diogelwch data personol achosi niwed a thrallod gwirioneddol i unigolion a gallant gynnig cyfle i gyflawni twyll hunaniaeth. Bydd y modd yr ymdrinnir â digwyddiadau o’r fath gan y Brifysgol yn lleihau ac yn cyfyngu ar yr effaith ar unigolion, ac mae rhoi gwybod yn gynnar am doriad yn hollbwysig er mwyn diogelu buddiannau’r unigolyn.

Ymhellach, mae rhwymedigaethau a osodir ar y Brifysgol o dan y Rheoliadau Diogelu Data Cyffredinol yn golygu bod yn rhaid rhoi gwybod am doriadau data personol i Swyddfa’r Comisiynydd Gwybodaeth o fewn 72 awr, ac y gallai methu â gwneud hynny arwain at osod dirwy o €10,000,000 ar y Brifysgol. Mae hi felly yn hollbwysig bod staff yn rhoi gwybod am bob toriad a’u bod yn gwneud hynny’n brydlon yn unol â’r weithdrefn hon.

I gael mwy o wybodaeth am ddiogelu data a diffiniadau o dermau allweddol, cyfeiriwch at y tudalennau diogelwch data ar The Hub.

**Pwrpas**

Mae’r weithdrefn hon yn hysbysu staff a’r rheiny sy’n trin data personol sy’n eiddo i’r Brifysgol o’r camau y mae’n rhaid iddynt eu cymryd os bydd data personol / system sy’n dal data personol yn cael ei cholli neu ei pheryglu.

Mae’r weithdrefn hon yn sicrhau ymagwedd gyson at drin ac ymateb i doriadau data a digwyddiadau diogelwch gwybodaeth yn y Brifysgol.

**Cwmpas**

Mae’r weithdrefn hon yn berthnasol i bob aelod staff, myfyriwr, gwirfoddolwr, contractwr ac asiant trydydd parti/prosesydd data sy’n trin gwybodaeth ac asedau gwybodaeth y Brifysgol.

**Data personol**

Y diffiniad o ddata personol yw gwybodaeth yn ymwneud ag unigolyn sydd wedi’i adnabod neu sy’n adnabyddadwy a gall gynnwys (ond nid yw wedi’i gyfyngu i):

* Gwybodaeth ffeithiol am unigolion megis dyddiad geni, rhif yswiriant gwladol, cyfrif banc, enw a chyfeiriad.
* Gwybodaeth sensitif megis iechyd, bywyd rhywiol, cofnod troseddol, ethnigrwydd, crefydd.
* Barnau a fynegwyd, er enghraifft, mewn adolygiadau datblygu staff neu mewn sylwadau mewn e-bost.

**Diffiniad o ddigwyddiad**

Y diffiniad o doriad diogelwch data personol yw:

“Toriad diogelwch sy’n arwain at ddinistrio, colli, newid, datgelu heb awdurdod neu gyrchu data personol sy’n cael ei drawsyrru, ei storio neu ei brosesu fel arall, yn ddamweiniol neu’n anghyfreithlon.”

Mae hyn yn cynnwys gwybodaeth ar bapur a gwybodaeth electronig. Mae toriadau’n cynnwys (ond nid ydynt wedi’u cyfyngu i):

* Lle collir mynediad i ddata personol sy’n cael ei ddal e.e. mae wedi cael ei ddinistrio, ei ddifrodi neu ei lygru yn gynamserol ac nid oes copïau eraill ar gael.
* Dwyn neu golli data e.e. colli papurau sensitif neu liniadur sy’n cynnwys data personol.
* Achosion o newid data personol mewn camgymeriad neu heb awdurdod.
* Datgelu damweiniol / datgelu anawdurdodedig e.e. data personol yn cael ei e-bostio i’r derbynnydd anghywir (yn fewnol neu’n allanol) neu’i gyhoeddi ar-lein / aelod staff yn defnyddio data personol a reolir gan y Brifysgol at bwrpas anawdurdodedig.
* Mynediad maleisus i ddata e.e. data personol myfyriwr yn cael ei roi i dwyllwr dros y ffôn neu hacio.
* Mynediad anawdurdodedig i system / cyfrif Prifysgol e.e. aelod staff yn datgelu ei gyfrinair i drydydd parti o ganlyniad i dwyll / gwe-rwydo.

**Camau i’w cymryd**

Pan ddarganfyddir toriad diogelwch, rhaid i’r aelod staff sydd wedi darganfod y toriad lenwi’r [**ffurflen**](https://forms.office.com/Pages/ResponsePage.aspx?id=fP6q5RuXt0qwORQa02rOwD5ufQVS6UhPjmkNXkFBMcdUQkJSOTFMMFFCOTVMSDNDWEFCSTIwWDRYWi4u) hon ar unwaith a darparu’r wybodaeth berthnasol. Rhaid rhoi gwybod am doriadau diogelwch i Wasanaethau TG ar unwaith a ddim hwyrach na 12 awr ar ôl i’r aelod staff ddod i wybod am y digwyddiad.

Os bydd rhywun yn amau bod toriad diogelwch wedi digwydd, dylai weithredu’n ofalus a chyflwyno adroddiad gan ddefnyddio’r ffurflen ar-lein.

Rhaid darparu’r wybodaeth a ganlyn:

* Esboniad o natur y toriad a’r ffactorau a arweiniodd at y toriad.
* Cadarnhad bod y toriad dan reolaeth.
* Beth yw natur y data (personol / personol sensitif a manylion y math o wybodaeth).
* Data pwy y mae’r toriad wedi effeithio arnynt – staff, myfyrwyr, ac ati.
* Faint o ddefnyddwyr yr effeithiwyd arnynt.
* Unrhyw gwynion a dderbyniwyd.
* Pa fesurau a gymerwyd i leddfu’r effeithiau.
* Faint o ddata / unigolion y mae’r toriad wedi effeithio arnynt.
* Pwy yw’r unigolion y mae’r toriad wedi effeithio ar eu data.
* Canlyniadau tebygol y toriad data.
* Manylion cysylltu’r aelod staff fel y gellir trafod y mater.
* Enw’r rheolwr llinell.

**Camau i’w cymryd gan y Brifysgol**

Ar ôl i’r Brifysgol dderbyn hysbysiad bod diogelwch data wedi’i dorri, bydd yn ystyried sut i ymateb yn unol â’r Weithdrefn Rheoli Digwyddiadau Diogelwch TG.

**Methiant i gydymffurfio â’r weithdrefn hon**

Byddai methu â rhoi gwybod am doriad data yn torri Polisi Diogelu Data’r Brifysgol a gallai aelodau staff gael eu disgyblu.

**Cysylltiadau â pholisïau a gweithdrefnau eraill**

Dylid darllen y ddogfen hon ar y cyd â:

Polisi Diogelu Data y Brifysgol

Y Rheoliadau TG

Y Weithdrefn Rheoli Digwyddiadau Diogelwch TG

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Fersiwn | Dyddiad cyhoeddi | Disgrifiad o’r adolygiad | Awdur | Cymeradwywyd gan a dyddiad | Dyddiad Adolygu Nesaf |
| 1.0 | Ionawr 2018 | Cyhoeddiad cyntaf | Rhys Davies |  | Rhagfyr 2019 |