



**DULLIAU GWEITHREDU AR GYFER RHEOLI ACHOS
A DYBIR SY’N TORRI DIOGELWCH DATA**

Dyddiad	Diben Cyhoeddi/Disgrifiad o’r Newid	Asesiad o'r Effaith ar Gydraddoldeb wedi'i Gwblhau
5 Hydref, 2009	Cyhoeddiad Cyntaf	
16 Gorffennaf 2018	Adolygu a diweddarau	

Swyddog Polisi	Uwch Swyddog Cyfrifol	Cymeradwywyd gan	Dyddiad
Pennaeth Llywodraethu a Chydymffurfio	Ysgrifennydd y Brifysgol	Grŵp Tasg Cydymffurfio	16 Gorffennaf 2018

Caiff y polisi hwn ei adolygu ymhen blwyddyn.

DULLIAU GWEITHREDU AR GYFER RHEOLI ACHOS A DYBIR SY’N TORRI DIOGELWCH DATA

1. Cyflwyniad

Dan ofynion Deddf Gwarchod Data 2018, mae'n orfodol rhoi gwybod am achos o fethu â gwarchod data os yw hynny'n debygol o arwain at risg i hawliau a rhyddid pobl. Rhaid rhoi gwybod am achosion o fethu â diogelu data i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr ar ôl i'r Brifysgol ddod i wybod amdanynt.

Rhaid i'r Brifysgol felly gymryd mesurau priodol yn erbyn prosesu data personol heb awdurdod neu'n anghyfreithlon, ac yn erbyn colli data personol drwy ddamwain, eu dinistrio neu eu difrodi.

Mae'r dulliau gweithredu hyn yn nodi sut bydd y Brifysgol yn rheoli achos y rhoddir gwybod iddynt a dybir sy'n torri diogelwch data.

Gall torri diogelwch data ddigwydd am nifer o resymau:

- Colli data neu offer ar yr hyn y cedwir y data, neu ladrad o'r cyfryw bethau
- Rheoliadau mynediad amhriodol sy'n caniatáu defnydd heb awdurdod
- Methiant offer
- Gwall dynol
- Amgylchiadau na ragwelwyd, fel tân neu lifogydd
- Ymosodiad hacio
- Troseddau 'blagio' lle ceir gwybodaeth drwy dwyllo'r sefydliad sy'n ei dal

Wrth reoli unrhyw achos a dybir o dorri diogelwch data, bydd y Brifysgol yn cymryd pedwar cam eglur:

1. Atal ac Adfer
2. Asesu Risgiau a hysbysiad pellach
3. Ystyried Hysbysiad Pellach
4. Gwerthuso ac Ymateb

2. Rhoi gwybod am Fethu â Diogelu Data

Rhaid rhoi gwybod am unrhyw achos a amheuir o fethu â diogelu data i'r Pennaeth Llywodraethu a Chydymffurfio, neu i Ysgrifennydd y Brifysgol, cyn gynted ag y gellir, ac yn sicr o fewn 24 awr, fel y gellir gweithredu'n briodol i atal y methiant ac adfer y sefyllfa.

3. Atal ac Adfer

Mae achosion a dybir sy'n torri diogelwch data yn gofyn am i'r Brifysgol ymchwilio i'r sefyllfa a'i hatal, a hefyd llunio cynllun adfer a fydd yn cynnwys, lle bo angen, unrhyw gyfyngiad ar ddifrod.

Ar ôl cael gwybod am achos a dybir sy'n torri diogelwch data, bydd y Pennaeth Llywodraethu a Chydymffurfio yn cymryd camau i archwilio, a bydd yn gwneud y canlynol yn benodol:

- Canfod pwy sydd angen cael gwybod am yr achos, a rhoi gwybod iddynt yr hyn y disgwylir iddynt ei wneud i gynorthwyo â'r ymarferiad atal. (Gall hyn gynnwys, er enghraifft, ynysu neu gau rhan o'r rhwydwaith a beryglwyd, cymryd camau i ganfod darn o offer sydd ar goll, neu newid y codau mynediad ar ddrws);

- Canfod a oes unrhyw beth i'w wneud i adfer unrhyw golledion a chyfyngu'r difrod y gallai'r achos o dorri diogelwch data ei achosi;
- Lle bo'n briodol, rhoi gwybod i'r heddlu.

4. Asesu Risgiau a hysbysiad pellach

Cyn penderfynu pa gamau eraill sydd eu hangen ar wahân i'r rhai a gymerwyd i atal yr achos ar unwaith, bydd Ysgrifennydd y Brifysgol, a'r Pennaeth Llywodraethu a Chydymffurfio, ar ran y Brifysgol, mewn ymgynghoriad â'r Deon Coleg, Pennaeth Ysgol ac/neu Gyfarwyddwr Gwasanaeth Proffesiynol perthnasol yn gwneud asesiad cychwynnol o'r risgiau a allai fod yn gysylltiedig â'r achos hwnnw.

Fel rhan o'r broses asesu hon, dylid ystyried p'un a oes angen rhoi gwybod am y digwyddiad i swyddfa'r Comisiynydd Gwybodaeth. Wrth wneud yr asesiad hwn, caiff y ffactorau canlynol eu hystyried:

- Pa fath o ddata sydd dan sylw?
- Pa mor sensitif ydyw?
- Os collwyd data neu os ydynt wedi cael eu lladrata, a oes unrhyw amddiffyniadau mewn grym megis amgryptio?
- Beth sydd wedi digwydd i'r data?
- Beth allai'r data ei ddweud wrth drydydd parti am yr unigolyn?
- Data personol faint o unigolion yr effeithir arnynt gan yr achos?
- Pwy yw'r unigolion y torrwyd diogelwch eu data?
- Pa niwed allai ddod i'r unigolion hynny? A oes risgiau i ddiogelwch corfforol neu enw da, neu risg colled ariannol, neu gyfuniad o'r rhain ac elfennau eraill o'u bywyd?
- A oes canlyniadau ehangach i'w hystyried, fel risg i iechyd y cyhoedd neu golli hyder y cyhoedd?

Dylai asesiad o ganlyniadau niweidiol posib i unigolion, pa mor ddifrifol neu sylweddol yw'r rhain a pha mor debygol ydynt o ddigwydd (e.e. colled ariannol, dwyn hunaniaeth neu dorri cyfrinachedd) hefyd ystyried y ffactorau canlynol, yn cynnwys rhoi gwybod i'r unigolion eu hunain:

- A oes unrhyw ofynion cyfreithiol neu gytundebol?
- A all hysbysu helpu'r Brifysgol i gyflawni ei rhwymedigaethau diogelwch o ran y chweched egwyddor diogelu data¹?
- A all hysbysu helpu'r unigolyn i reoli'r risgiau, er enghraifft, drwy ganslo cerdyn credyd neu newid cyfrinair?
- Sut gellir gwneud hysbysu'n briodol ar gyfer grwpiau penodol o unigolion, er enghraifft, plant neu oedolion agored i niwed.
- Pwy fydd y Brifysgol yn eu hysbysu, beth ddywedir wrthynt a sut y rhoddir y neges iddynt?
- Pwy arall ddylid eu hysbysu, er enghraifft trydydd parti fel yr heddlu, yswirwyr, cyrdd proffesiynol, banc neu gwmnïau cardiau credyd.

Ar ddiwedd y cam hwn bydd y Pennaeth Llywodraethu a Chydymffurfio yn ysgrifennu adroddiad llawn o'r prosesau asesu a gyflawnwyd hyd yma, a chyflwynir hwnnw i'r Grŵp Gwerthuso fel yr amlinellir yn Adran 5 isod.

1 Proseswyd mewn ffordd sy'n sicrhau diogelwch priodol y data personol

Os penderfynir bod angen hysbysu Swyddfa'r Comisiynydd Gwybodaeth am y digwyddiad, dylai'r Pennaeth Llywodraethu a Chydymffurfio wneud hynny ar ddiwedd y cam hwn, a beth bynnag o fewn 72 awr i gael gwybod am yr achos dan sylw.

5. Gwerthuso ac Ymateb

Mae'r Brifysgol yn cydnabod ei bod yn bwysig nid yn unig i ymchwilio i achosion unrhyw dorri diogelwch data, ond hefyd gwerthuso effeithiolrwydd ymateb y Brifysgol iddynt.

Bydd y Pennaeth Llywodraethu a Chydymffurfio yn galw *Grŵp Gwerthuso* ynghyd gyda chyfansoddiad craidd yn cynnwys:

- Cadeirydd y Grŵp Tasg Cydymffurfio, fydd yn dod yn Gadeirydd y Grŵp Gwerthuso
- Pennaeth Llywodraethu a Chydymffurfio
- Y Deon Coleg, Pennaeth Ysgol a / neu Gyfarwyddwr Gwasanaeth Proffesiynol priodol a bennir gan natur y torri diogelwch data
- Rheolwyr gweithredol perthnasol a bennir gan natur y torri diogelwch data.

Wrth lunio ei gasgliadau, bydd y Grŵp Gwerthuso'n cymryd i ystyriaeth y materion allweddol a ganlyn mewn perthynas â'r torri diogelwch data:

- Beth yw'r gwersi sydd i'w dysgu?
- A all y Brifysgol fodloni ei hun ei bod yn gwybod pa ddata personol a gedwir ac ymhle a sut cânt eu cadw?
- Mewn cysylltiad â data personol, beth ac ymhle mae'r risgiau mwyaf i'r sefydliad? Er enghraifft, ymhle cedwir data categori arbennig?
- A yw'r risgiau'n gysylltiedig â rhannu neu ddatgelu data wedi eu nodi a'u rheoli'n addas?
- Beth yw'r pwyntiau gwan posibl ym mesurau diogelwch presennol y Brifysgol – fel defnyddio dyfeisiadau storio cludadwy?
- Sut mae ymwybyddiaeth staff o faterion diogelwch yn cael ei fonitro, a llenwi unrhyw fylchau drwy hyfforddiant neu gyngor wedi'i addasu'n arbennig.

Dylai Cadeirydd y Grŵp Gwerthuso gyflwyno adroddiad llawn i'r Grŵp Tasg Cydymffurfio yn ei gyfarfod nesaf, yn cynnwys unrhyw argymhellion allai gynnwys gweithredu yn unol â Threfn Disgyblu'r Brifysgol.