TYFU CYMRU
GROW WALES

12 Cam at gydymffurfio â GDPR

ANNA BEZODIS
TRAINING AND CONSULTANCY

Cronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig: Ewrop yn Buddsoddi mewn Ardaloedd Gwledig
European Agricultural Fund for Rural Development: Europe Investing in Rural Areas
Llywodraeth Cymru
Welsh Government

Mae TyfuCymru wedi derbyn cyllid drwy Gymunedau Gwledig Llywodraeth Cymru – Rhaglen Datblygu Gwledig 2014-2020, sy'n cael ei hariannu gan Gronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig a Llywodraeth Cymru.

TyfuCymru
Lantra Cymru, Maes y Sioe Frenhinol,
Llanfair-ym-Muallt LD2 3WY
Ff:+44 (0)1982 552646
E: tyfucymru@lantra.co.uk
G: www.tyfucymru.co.uk

Arweinir TyfuCymru gan Lantra Cymru sy'n gwmni sydd wedi'i gofrestru yng Nghymru a Lloegr.
Rhif cofrestredig: 2823181
Rhif elusen: 1022991
Rhif TAW: 585 3815 08

Cyflwyniad

Os ydych yn casglu neu'n derbyn data personol a bod gennych **reolaeth** dros pam mae angen y data hwnnw arnoch a sut y dylid ei ddefnyddio, ystyrir eich bod yn **rheolydd data**. Neu os ydych yn **prosesu** data personol ar ran rheolydd data, byddwch yn cael eich ystyried fel **prosesydd data**. Yn y naill achos neu'r llall, mae angen i chi a'r rhai o fewn eich sefydliad weithio yn unol â'r rheolau a nodir yn neddfwriaeth GDPR y DU, er mwyn cydymffurfio'n gyfreithiol.

Beth sy'n cael ei ystyried yn 'ddata personol'?

Mae data personol yn cynnwys gwybodaeth fel:

- enw neu fanylion cyswllt person (gelwir y person hwn yn 'wrthrych y data')
- rhif adnabod, er enghraifft rhif Yswiriant Gwladol neu basbort person
- data lleoliad, er enghraifft cyfeiriad cartref neu ddata GPS ffôn symudol unigolyn
- dynodydd ar-lein, er enghraifft cyfeiriad IP neu e-bost person.

Mae GDPR y DU hefyd yn ymdrin â data personol yr ystyrir ei fod yn fwy sensitif, a chyfeirir ato fel 'datacategori arbennig'. Mae data categori arbennig yn cynnwys yn benodol:

- data genetig sy'n ymwneud â nodweddion genetig sy'n rhoi gwybodaeth unigryw am ffisioleg neu iechyd person
- data biometrig at ddiben adnabod person, gan gynnwys delweddau wyneb ac olion bysedd
- data sy'n ymwneud ag iechyd corfforol neu feddyliol person, a darpariaeth gwasanaethau gofal iechyd
- tarddiad hiliol neu ethnig
- barn wleidyddol
- credoau crefyddol neu athronyddol
- aelodaeth undebau llafur
- bywyd rhywiol neu gyfeiriadedd rhywiol.

(Ffynhonnell: https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-a4T2s2Y2ffXd#what-is-personal-data)

Dyma restr dasgau 12 cam i'ch helpu i gydymffurfio â GDPR y DU:

CAM 1

Cofrestrwch gyda Swyddfa'r Comisiynydd Gwybodaeth (ICO) a thalu ffi gofrestru, oni bai eich bod wedi'ch eithrio rhag gwneud hynny. Os nad ydych yn siŵr a oes angen i chi gofrestru, mae gan Swyddfa'r Comisiynydd Gwybodaeth gwis hunanasesu i'ch helpu i benderfynu ar eich statws.

CAM 2

Bydd angen i chi archwilio a dogfennu'r data sydd gennych.

Gellir lawrlwytho templedi dogfennaeth yma!

Gall y cwestiynau i'w gofyn gynnwys:

• **Pwy** yw gwrthrychau'r data? Pwy sydd â mynediad at ddata categori personol neu arbennig?
• **Ble** rydyn ni'n cadw data personol? I ble / at bwy rydyn ni'n trosglwyddo data personol?
• **Pam** ydyn ni'n prosesu data personol (beth yw'r diben)? Pam ydym yn ei rannu â thrydydd partïon?
• **Pa** fecanweithiau sydd gennym ar waith i ddiogelu data personol? Pa sail/seiliau cyfreithlon ydym yn dibynnu arnynt i brosesu data?
• **Sut** mae data'n cael ei brosesu? Am ba hyd y dylid ei gadw?

(Ffynhonnell: https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-a4T2s2Y2ffXd#what-is-personal-data)

CAM 3

O'r archwiliad data a gynhaliwyd yng NGHAM 2, nodwch unrhyw feysydd risg, a rhowch fesurau diogelwch ar waith i reoli'r risgiau hynny.

Mae'r gyfraith yn mynnu bod gennych lefel o ddiogelwch sy'n 'briodol' i'r risgiau a gyflwynir gan eich prosesau data.

Ar y templedi dogfennaeth mae colofnau i'w cwblhau (gweler ail dab y daenlen am enghreifftiau defnyddiol!).

CAM 4

Deall pryd mae angen Asesiad Effaith Diogelu Data (DPIA). Mae DPIA yn broses i'ch helpu i nodi a lleihau risgiau diogelu data prosiect, a rhaid i chi wneud DPIA cyn i chi ddechrau unrhyw fath o brosesu data sy'n debygol o arwain at risg uchel i unigolion.

I gael rhagor o wybodaeth am hyn, ac i gael mynediad at ddogfen DPIA enghreifftiol, dilynwch y ddolen yma!

CAM 5

Crëwch/diweddarwch eich polisi diogelu data (y gellid cyfeirio ato hefyd fel eich 'polisi preifatrwydd') a sicrhewch ei fod yn adlewyrchu unrhyw newidiadau rydych wedi'u gwneud yn unol â GDPR y DU.

Gellir dod o hyd i nodiadau canllaw defnyddiol ar sut i greu polisi diogelu data yma!

Nid yw'n hanfodol bod gennych un, OND mae angen i chi roi gwybod i bobl beth rydych chi'n mynd i'w wneud â'u data personol (gan ddefnyddio hysbysiad preifatrwydd – Gweler CAM 6).

CAM 6

Wrth brosesu data personol, rhaid i chi ddweud wrth bobl beth rydych chi'n ei wneud ag ef. Mae ganddynt yr hawl i wybod gwybodaeth allweddol fel pam mae ei hangen arnoch, beth fyddwch chi'n ei wneud ag ef a gyda phwy rydych chi'n mynd i'w rannu. Dylech ddarparu'r wybodaeth hon mewn ffordd glir, agored a gonest.

Mae'n well ysgrifennu hyn mewn dogfen o'r enw hysbysiad preifatrwydd.

Gellir lawrlwytho templed rhybudd preifatrwydd yma!

CAM 7

Ydych chi'n dibynnu ar gael caniatâd person i brosesu ei ddata personol? Dim ond un o'r seiliau cyfreithlon y gallwch ddibynnu arno yw caniatâd, felly ni fydd angen caniatâd arnoch bob amser ond mae rhai achosion lle mai dyma fydd yr opsiwn gorau.

Os ydych yn dibynnu ar ganiatâd, adolygwch sut y byddwch yn ei geisio, ei gofnodi a'i reoli.

O dan GDPR y DU, er mwyn i ganiatâd fod yn ddilys, rhaid iddo gael ei roi'n rhydd, rhaid iddo fod yn benodol am yr hyn y mae'r person yn cydsynio iddo, rhaid iddo fod yn glir, rhaid optio i mewn (ni allwch ddefnyddio blychau wedi'u ticio ymlaen llaw na dibynnu ar ganiatâd 'optio allan' diofyn), rhaid iddo fod wedi'i ddogfennu'n briodol a rhaid gallu ei dynnu'n ôl yn hawdd.

Efallai y bydd angen i chi ofyn am ganiatâd newydd sy'n cydymffurfio â GDPR y DU os nad yw eich caniatadau presennol yn bodloni'r safon ofynnol, neu os ydynt wedi'u dogfennu'n wael.

Cliciwch yma am restr wirio ddefnyddiol i sicrhau bod eich dull o ofyn am ganiatâd, ei gofnodi a'i reoli yn cydymffurfio.

CAM 8

A oes angen swyddog diogelu data ar eich sefydliad?

Mae gan Swyddfa'r Comisiynydd Gwybodaeth gwis hunanasesu 5 munud o hyd i'ch helpu chi i benderfynu a oes angen i chi benodi swyddog diogelu data yn gyfreithlon ai peidio.

CAM 9

Ystyriwch sut y gallwch gydymffurfio â data prosesu yn unol â hawliau'r unigolyn – e.e. ymateb i gais i ddileu data, neu drosglwyddo data yn unol â'r hawl i gludadwyedd data.

CAM 10

Byddwch yn barod am dorri diogelwch data personol! Gallwn i gyd wneud camgymeriadau, felly gwnewch yn siŵr eich bod yn nodi gweithdrefnau y gallwch eu rhoi ar waith i ganfod achosion o dorri diogelwch cyn gynted â phosibl. Efallai y bydd angen i chi roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am dorri diogelwch data personol, felly mae'n bwysig iawn bod pawb yn eich sefydliad yn gwybod sut i adnabod a thynnu sylw at unrhyw achosion o dorri diogelwch data sy'n digwydd.

Mae gan Swyddfa'r Comisiynydd Gwybodaeth restrau gwirio ar gael ar sut i baratoi ar gyfer torri diogelwch data ac ymateb iddo, sydd i'w weld yma!

CAM 11

Diweddarwch eich gweithdrefnau ar gyfer ymdrin ag unrhyw Gais Gwrthrych am Wybodaeth.

CAM 12

Hyfforddwch staff, gwirfoddolwyr a/neu weithwyr dros dro i sicrhau eu bod yn gwybod i gadw at eich systemau/prosesau. Darparwch restrau gwirio a/neu ddogfennau canllaw a allai helpu gyda chydymffurfio o ddydd i ddydd.

Crynodeb o'r Rhestr Dasgau

- Cofrestru gyda Swyddfa'r Comisiynydd Gwybodaeth
- Cynnal archwiliad data
- Nodi risgiau (a'u dogfennu)
- Deall pryd mae angen Asesiadau Effaith Diogelu Data
- Creu/diweddaru eich polisi diogelu data
- Adolygu/diweddaru hysbysiadau preifatrwydd
- Adolygu sut y byddwch yn ceisio, yn cofnodi ac yn rheoli caniatâd
- Penderfynu a oes angen i chi benodi Swyddog Diogelu Data yn gyfreithiol
- Ystyried sut y gallwch sicrhau eich bod yn prosesu data yn unol â hawliau unigolyn
- Nodi gweithdrefnau i baratoi ar gyfer torri diogelwch data ac ymateb iddo
- Diweddaru eich gweithdrefnau ar gyfer ymdrin â Chais Gwrthrych am Wybodaeth
- Darparu hyfforddiant a rhestrau gwirio/nodiadau cyfarwyddyd i helpu eich staff neu wirfoddolwyr i brosesu data mewn ffordd sy'n cydymffurfio