Cyngor Trydydd Sector Caerdydd

Eich cyngor gwirfoddol sirol lleol

2. Rheoli eich sefydliad

2.12 Diogelu data a GDPR

Cardiff Third Sector Council
Cyngor Trydydd Sector Caerdydd

Beth yw'r Rheoliad Diogelu Data Cyffredinol (GDPR)?

Deddf Ewropeaidd sydd wedi'i chyflwyno i gryfhau ac uno diogelu data i unigolion o fewn yr Undeb Ewropeaidd.
Ar hyn o bryd, mae'n ofynnol i'r Deyrnas Unedig gydymffurfio â Deddf Diogelu Data 1998 (a Chyfarwyddeb Diogelu Data yr UE 1995), ond o 25ain Mai 2018 ymlaen bydd angen i holl aelod-wladwriaethau'r UE gydymffurfio â'r GDPR yn hytrach.
Bydd Swyddfa'r Comisiynydd Gwybodaeth (ICO) yn rheoleiddio gweithrediad y GDPR yn y DU.

I ba fath o wybodaeth y mae'r GDPR yn berthnasol?

Fel Deddf Diogelu Data 1998, mae'r GDPR yn berthnasol i 'ddata personol', ond mae'r diffiniad o ddata personol wedi'i ehangu. O dan y GDPR, mae data personol yn golygu unrhyw wybodaeth yn ymwneud â pherson byw adnabyddadwy y gellir ei adnabod yn uniongyrchol *neu'n anuniongyrchol* o'r wybodaeth honno.
Mae hefyd yn berthnasol i ddata personol sensitif, y mae'r GDPR yn ei alw'n 'ddata categori arbennig'. Ceir mesurau ychwanegol i warchod y categorïau hynny, ac mae'n cynnwys data sy'n ymwneud â hil neu darddiad ethnig, crefydd, iechyd, a geneteg unigolyn. Mae biometreg hefyd bellach wedi'i chynnwys os defnyddir y data hwnnw i adnabod unigolyn yn benodol. Nid yw data yn ymwneud ag euogfarnau neu droseddau yn ddata categori arbennig, ond ceir mesurau diogelu ar wahân ar gyfer y math hwn o ddata o fewn Erthygl 10 yn y GDPR.

A fydd angen i mi gydymffurfio â'r GDPR?

Os ydych yn gweithio neu'n gwirfoddoli i fudiad neu fusnes sy'n prosesu data personol, yna mae'n debygol y bydd angen i chi gydymffurfio â'r GDPR.
Nid oes gwahaniaeth a ydych wedi'ch lleoli o fewn un o aelod-wladwriaethau'r UE ai peidio: os yw'ch mudiad yn prosesu data personol yn ymwneud â thrigolion yr UE, ac ystyrir ei fod naill ai'n 'rheolydd data' neu'n 'brosesydd data', bydd angen i'ch mudiad gydymffurfio â'r GDPR.

Rheolydd data yw'r mudiad neu'r person (megis unig fasnachwr) sy'n casglu ac yn defnyddio data personol, ac yn pennu dibenion a dulliau prosesu'r data hwnnw.
Prosesydd data yw'r mudiad neu'r person sy'n gyfrifol am brosesu data personol ar ran rheolydd data. Gallai hyn gynnwys mudiadau sy'n darparu gwasanaethau megis rheoli cyflogres, anfon gohebiaeth, systemau TG, a gwaredu gwastraff cyfrinachol.

Mae'r GDPR yn rhoi rhwymedigaethau cyfreithiol penodol ar broseswyr data nad ydynt yn bodoli o dan y Ddeddf Diogelu Data, a bydd gan broseswyr bellach atebolrwydd cyfreithiol os ydynt yn gyfrifol am fethiant yn ymwneud â data.

Sut mae'r GDPR yn wahanol i'r Ddeddf Diogelu Data?

Mae llawer o nodweddion tebyg rhwng y ddwy ddeddfwriaeth, ond mae'r GDPR wedi cyflwyno nifer o ddarpariaethau newydd y bydd angen i chi fod yn ymwybodol ohonynt.

Egwyddorion

Mae nifer yr egwyddorion diogelu data wedi'i leihau o 8 i 6, ond maent yn dal yn debyg iawn o ran eu cynnwys i'r 8 egwyddor a nodir yn y Ddeddf Diogelu Data. Dywed y 6 egwyddor diogelu data a nodir yn y GDPR fod yn rhaid cadw at y canlynol:

1. prosesu data yn gyfreithlon, yn deg ac yn dryloyw mewn perthynas ag unigolion;
2. casglu data at ddibenion cyfreithlon a phenodol sydd wedi'u nodi'n glir, a pheidio â'i brosesu mewn unrhyw ffordd sy'n anghyson â'r dibenion hynny;
3. rhaid i ddata fod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol ar gyfer y dibenion y mae'n cael ei brosesu ar eu cyfer;
4. rhaid i ddata fod yn gywir, a'i ddiweddaru pan fo angen;
5. rhaid cadw data mewn dull sy'n caniatáu adnabod gwrthrychau data, am ddim mwy nag sy'n angenrheidiol at y dibenion y mae'r data personol yn cael ei brosesu ar eu cyfer;
6. rhaid prosesu data mewn modd sy'n sicrhau diogelwch priodol y data personol, gan ddefnyddio mesurau technegol neu sefydliadol priodol.

Mae'r GDPR hefyd yn cyflwyno egwyddor atebolrwydd gyffredinol. Mae'r egwyddor hon yn ei gwneud yn ofynnol i reolyddion data fod yn gyfrifol am gydymffurfio â'r 6 egwyddor a nodir uchod, a gallu dangos eu bod yn cydymffurfio.

Hysbysiadau preifatrwydd

Datganiad yw hysbysiad preifatrwydd yr ydych yn ei ddarparu i unigolion wrth i chi gasglu gwybodaeth ganddynt, gan egluro'r hyn mae angen iddynt ei wybod ynglŷn â diogelu data. Mae'r GDPR yn cyflwyno gofyniad i ddarparu hysbysiadau preifatrwydd manylach i unigolion wrth gasglu data personol, gan gynnwys gwybodaeth megis:

- at ba ddiben(ion) y bydd y data personol yn cael ei brosesu
- y sail gyfreithlon y mae'r mudiad yn dibynnu arni i brosesu data yr unigolyn dan sylw (gweler isod)
- am ba mor hir y bydd y data yn cael ei gadw
- â phwy y bydd neu y gallai'r data gael ei rannu
- hawl yr unigolyn i dynnu caniatâd yn ôl os yw'n dymuno gwneud hynny.

Mae manylion pellach ynghylch y wybodaeth y mae angen i chi ei darparu i unigolion ar gael ar wefan yr ICO.

Swyddogion Diogelu Data

O dan y GDPR, bydd angen i'ch mudiad benodi'n gyfreithiol Swyddog Diogelu Data os ydych yn ateb y meini prawf canlynol:

- rydych yn awdurdod cyhoeddus;

- mae'ch gweithgareddau craidd yn ei gwneud yn ofynnol i chi fonitro unigolion ar raddfa fawr, yn rheolaidd ac yn systematig (er enghraifft, olrhain ymddygiad arlein); neu
- mae'ch gweithgareddau craidd yn cynnwys prosesu, ar raddfa fawr, ddata categori arbennig neu ddata yn ymwneud ag euogfarnau a throseddau.

Os nad ydych yn ateb y meini prawf hyn, gallwch benodi Swyddog Diogelu Data o'ch gwirfodd os mynnwch, ond sylwch fod yr un gofynion mewn grym ar gyfer y rôl a'r tasgau â'r gofynion sy'n bodoli pan fo penodi Swyddog Diogelu Data yn orfodol. Fel arall, gallwch benodi rhywun i fod yr 'arweinydd' diogelu data (neu deitl tebyg) yn eich mudiad, i gydlynu darpariaethau diogelu data o fewn eich mudiad, ac o bosib weithredu fel y person y mae staff a/neu wirfoddolwyr yn adrodd unrhyw fethiannau data iddo, ond ni fydd angen i chi gadw at y gofynion swyddogol sy'n gysylltiedig â rôl y Swyddog Diogelu Data.

Mae gwybodaeth ychwanegol ynglŷn â meini prawf a manylion rôl y Swyddog Diogelu Data ar gael yng nghanllaw'r ICO ar y GDPR, ac yn y ddogfen Cwestiynau Cyffredin hon.

Cryfhau hawliau

Mae'r Ddeddf Diogelu Data yn rhoi hawliau amrywiol i unigolion mewn perthynas â'u data personol, ond mae'r GDPR yn cryfhau'r hawliau hynny, ac yn cynnwys hawl newydd yn ymwneud â chludadwyedd data. Mae'r GDPR yn rhoi'r hawliau canlynol i unigolion:

1. Yr hawl i gael gwybod
2. Yr hawl i gael mynediad
3. Yr hawl i gywiriad
4. Yr hawl i ddilead (a elwir hefyd yr hawl i gael eich anghofio)
5. Yr hawl i gyfyngu ar brosesu
6. Yr hawl i gludadwyedd data
7. Yr hawl i wrthwynebu
8. Hawliau yn ymwneud â phenderfynu a phroffilio awtomataidd.

Mae manylion llawn ynghylch pob un o'r hawliau hyn ar gael ar wefan yr ICO.

Sail gyfreithlon dros brosesu data

Cyn y gallwch brosesu unrhyw ddata personol, mae'r GDPR yn ei gwneud yn ofynnol i chi bennu sail gyfreithlon ddilys i allu ei brosesu. Mae 6 sail y gallwch ddewis dibynnu arnynt, a bydd angen i chi bennu pa un neu fwy o'r rhain sy'n berthnasol i'ch gweithgareddau prosesu data. Gall teclyn rhyngweithiol yr ICO ar gyfer y sail gyfreithlon fod o gymorth gyda hyn.

Dyma'r 6 sail gyfreithlon sydd ar gael i brosesu data:

(a) Caniatâd: mae'r unigolyn wedi rhoi caniatâd clir i chi brosesu ei ddata personol i bwrpas penodol (gweler isod am ragor o fanylion)

(b) Contract: mae angen y prosesu ar gyfer contract sydd gennych â'r unigolyn, neu gan ei fod wedi gofyn i chi gymryd camau penodol cyn ymrwymo i gontract
(c) Rhwymedigaeth gyfreithiol: mae angen y prosesu fel eich bod yn cydymffurfio â'r gyfraith (ond nid yw hyn yn cynnwys unrhyw rwymedigaethau contractiol sydd gennych)
(d) Buddiannau hanfodol: mae angen y prosesu i ddiogelu bywyd rhywun
(e) Tasg gyhoeddus: mae angen y prosesu er mwyn gallu cyflawni tasg sydd o fudd cyhoeddus neu ar gyfer eich swyddogaethau swyddogol, ac mae gan y dasg neu'r swyddogaeth sail glir o dan y gyfraith (mae hyn yn berthnasol yn bennaf i awdurdodau lleol, ond gall fod yn berthnasol i unrhyw fudiad sy'n arddel awdurdod swyddogol neu'n cyflawni tasgau sydd o fudd cyhoeddus)
(f) Buddiannau cyfreithlon: mae angen y prosesu ar gyfer buddiannau cyfreithlon eich mudiad, neu fuddiannau cyfreithlon trydydd parti, oni bai fod rheswm da dros ddiogelu data personol yr unigolyn sy'n cael blaenoriaeth ar y buddiannau cyfreithlon hynny.

Caniatâd

O dan y Ddeddf Diogelu Data, os ydych yn dibynnu ar ganiatâd i brosesu data personol unigolyn, fel arfer gallwch ddibynnu naill ai ar ganiatâd penodol (pan fo'r unigolyn yn optio i mewn i chi ddefnyddio ei ddata mewn ffyrdd penodol), neu ganiatâd awgrymedig (pan nad yw'r unigolyn yn optio allan o'ch defnydd o'i ddata).
Os ydych am ddibynnu ar ganiatâd fel y sail gyfreithlon dros brosesu data personol unwaith y daw'r GDPR i rym, ni fyddwch mwyach yn gallu dibynnu ar ganiatâd awgrymedig. Bydd yn rhaid iddo fod yn ganiatâd 'optio i mewn', sydd wedi'i roi o wirfodd, sy'n benodol ac sydd wedi'i seilio ar wybodaeth. Mae hyn yn golygu bod y trothwy ar gyfer caniatâd yn uwch o dan y GDPR, felly efallai y bydd angen i chi newid y ffordd yr ydych yn cael caniatâd gan unigolion (*os* oes angen caniatâd i chi brosesu eu data), a/neu efallai y bydd angen i chi gael caniatâd o'r newydd gan unigolion os na fydd y caniatâd sydd gennych ar hyn o bryd yn cydymffurfio â'r GDPR.
Mae'r ICO wedi cyhoeddi canllaw ar ganiatâd, sy'n cadarnhau'n union pa feini prawf y mae angen eu hateb er mwyn i ganiatâd fod yn ddilys o dan y GDPR. Sylwch, serch hynny, mai dim ond un o'r 6 opsiwn sydd ar gael i chi brosesu data personol yw caniatâd, ac efallai y bydd yn fwy priodol a/neu ymarferol i chi ddibynnu ar sail gyfreithlon wahanol i brosesu'r data yn lle caniatâd.

Adrodd methiannau

O dan y Ddeddf Diogelu Data, doedd dim rhwymedigaeth gyfreithiol i reolyddion data adrodd methiannau diogelwch, ond mae'r GDPR yn cyflwyno dyletswydd ar *bob* mudiad i adrodd methiant yn ymwneud â data personol i'r ICO *os* ydynt yn credu ei fod yn debygol o beryglu hawliau a rhyddidau'r unigolyn neu'r unigolion y mae eu data yn rhan o'r methiant hwnnw.

Os yw'r mudiad yn credu bod perygl o'r fath yn debygol, bydd angen ei adrodd i'r ICO cyn pen 72 awr ar ôl dod yn ymwybodol o'r methiant (os yw'n ymarferol i wneud hynny). Ac os yw'r methiant yn debygol o arwain at berygl *uchel* i hawliau a rhyddidau'r unigolyn neu'r unigolion y mae eu data yn rhan o'r methiant, bydd angen i'ch mudiad hefyd roi gwybod i'r unigolion hynny am y methiant heb oedi diangen.

O safbwynt ymarferol, mae hyn yn golygu bod angen i bob un o'ch staff a/neu'ch gwirfoddolwyr allu adnabod methiant os oes un yn digwydd, ac mae angen iddynt wybod hefyd i bwy i roi gwybod am fethiant o'r fath ar unwaith, fel y gellir anfon adroddiad at yr ICO cyn pen 72 awr os oes angen. Gellir osgoi'r rhan fwyaf o fethiannau data drwy roi mesurau diogelwch cadarn yn eu lle yn eich mudiad drwyddo draw.

Mae rhagor o wybodaeth ynglŷn â methiannau data a diogelwch ar gael ar wefan yr ICO.

Asesiadau Effaith Diogelu Data

Ers peth amser, mae'r ICO wedi bod yn annog rheolyddion data i gynnal Asesiadau Effaith Diogelu Data wrth weithio ar brosiectau sy'n cynnwys data personol. Yn ei hanfod, proses yw Asesiad Effaith Diogelu Data i ddadansoddi'ch gweithgareddau prosesu data, a'ch helpu i ganfod a lleihau risgiau diogelu data. Bydd y GDPR yn ei gwneud yn ofynnol i gynnal Asesiadau Effaith Diogelu Data ar gyfer mathau penodol o brosesu data, neu os yw prosesu data unigolyn yn debygol o arwain at berygl uchel i fuddiannau'r unigolyn hwnnw.

Mae'r ICO wedi datgan bod hyn yn elfen allweddol o'r pwyslais newydd ar atebolrwydd a 'diogelu data drwy ddylunio' o dan y GDPR, ynghyd â dull o gydymffurfio sydd wedi'i seilio'n fwy ar risg.

Mae gwybodaeth fanwl ynglŷn â sut i gynnal Asesiad Effaith Diogelu Data (os oes angen i chi gynnal un) ar gael yng nghanllaw'r ICO ar y GDPR, ynghyd â nifer o restrau gwirio a all fod o gymorth.

Dirwyon

O dan y Ddeddf Diogelu Data, mae gan yr ICO y grym i roi dirwyon gwerth hyd at £500,000 am fethiannau yn ymwneud â data personol. Mae'r GDPR yn cynyddu lefel y dirwyon hynny, a gallai'r ddirwy uchaf fod hyd at €20 miliwn (tua £17m) neu 4% o drosiant byd-eang (pa bynnag un sydd fwyaf). Serch hynny, mae'r ICO wedi cadarnhau na fydd ond yn rhoi dirwyon pan fo pob cam arall wedi methu, fel y gwna ar hyn o bryd. Ynghyd â'r grym i roi dirwyon uwch os yw'n teimlo bod hynny'n angenrheidiol, bydd yr ICO yn dal i allu rhoi sancsiynau eraill gan gynnwys rhybuddion, ceryddon a gorchmynion unioni.

Beth allaf ei wneud i sicrhau bod fy mudiad yn cydymffurfio â'r GDPR?

Mae nifer o gamau ymarferol y gallwch eu cymryd i geisio sicrhau bod eich mudiad yn cydymffurfio â'r GDPR, o 25 Mai 2018 ymlaen ac yn y dyfodol, gan gynnwys:

- Cynnal archwiliad i bennu pa ddata personol rydych yn ei ddal a beth rydych yn ei wneud gydag ef, ac yna gynnal asesiadau risg yn ymwneud â'r data hwnnw fel y gallwch roi mesurau yn eu lle i reoli unrhyw risgiau rydych yn eu canfod. Mae gan yr ICO nifer o dempledi a rhestrau gwirio a all fod o gymorth
- Pennu a yw'ch mudiad yn rheolydd data neu'n brosesydd data (neu'r ddau), ac adolygu unrhyw gytundebau ysgrifenedig sydd gennych gyda rheolyddion data neu broseswyr data i sicrhau eu bod yn cyd-fynd â'r darpariaethau newydd o fewn y GDPR
- Os ydych yn dibynnu ar ganiatâd i brosesu data personol unrhyw unigolion, dylid sicrhau ei fod yn cyrraedd y trothwy uwch o dan y GDPR
- Adolygu'ch hysbysiadau preifatrwydd a sicrhau eu bod yn cynnwys y manylion ychwanegol sy'n ofynnol o dan y GDPR
- Hyfforddi staff, gwirfoddolwyr a gweithwyr dros dro mewn diogelu data, a rhoi polisïau a gweithdrefnau ar waith yn eich mudiad drwyddo draw i sicrhau bod data yn cael ei brosesu yn unol ag egwyddorion diogelu data
- Pennu a oes angen i chi benodi Swyddog Diogelu Data
- Rhoi systemau yn eu lle i ganfod methiannau a rhoi gwybod i'r ICO amdanynt, pan fo angen.

Gwybodaeth bellach

Swyddfa'r Comisiynydd Gwybodaeth (ICO)
Ffôn: 0303 123 1113
www.ico.org.uk

Cynhyrchwyd y daflen wybodaeth hon gan Anna Bezodis Training and Consultancy:
www.annabezodis.com

Ymwadiad
Mae'r wybodaeth a ddarperir yn y daflen hon ar gyfer cyfarwyddyd yn unig. Nid yw'n amnewid am gyngor proffesiynol ac ni allwn dderbyn unrhyw gyfrifoldeb am golled o ganlyniad i unrhyw berson weithredu neu wrthod gweithredu arno.

Am rhagor o wybodaeth cysylltwch â

Cyngor Trydydd Sector Caerdydd
Tŷ Baltic, Sgwâr Mount Stuart , Caerdydd, CF10 5FH
Elusen Gofrestredig: *1068623*

Ffôn: 029 2048 5722 enquiries@c3sc.org.uk
Ffacs: 029 2046 4196 www.c3sc.org.uk

Cynhyrchwyd gan WCVA, Cynghorau Gwirfoddol Sirol a Chanolfannau Gwirfoddoli
Wedi ei ddiweddaru:11/06/2018

Ffôn: 0300 111 0124
www.wcva.org.uk