Diogelu Data a’r GDPR

Trosolwg

Beth yw’r Rheoliad Cyffredinol ar Ddiogelu Data (GDPR)?

Mae’n gyfraith Ewropeaidd sydd wedi’i chyflwyno i gryfhau ac uno diogelu data ar gyfer unigolion o fewn yr UE. Yn flaenorol, roedd yn ofynnol i’r DU gydymffurfio â Deddf Diogelu Data 1998 (a Chyfarwyddeb Diogelu Data’r UE 1995), ond o 25 Mai 2018 mae angen i bob un o aelod-wladwriaethau’r UE gydymffurfio â’r GDPR yn lle.

Bydd Swyddfa’r Comisiynydd Gwybodaeth (ICO) yn rheoleiddio’r broses o weithredu’r GDPR yn y DU.

Pa fath o wybodaeth y mae’r GDPR yn berthnasol iddi?

Fel Deddf Diogelu Data 1998, mae’r GDPR yn berthnasol i ‘ddata personol’, ond mae’r diffiniad ar gyfer y data hwnnw wedi’i ehangu.

Diffiniad – O dan y GDPR, ystyr data personol yw unrhyw wybodaeth sy’n ymwneud â pherson byw adnabyddadwy y gellir nodi pwy ydyw yn uniongyrchol neu’n anuniongyrchol o’r wybodaeth honno.

Mae hefyd yn berthnasol i ddata personol sensitif, y mae’n cyfeirio ati fel ‘data categori arbennig’. Mae’r categorïau hynny’n destun amddiffyniadau ychwanegol, ac yn cynnwys data sy’n ymwneud â hil neu darddiad ethnig, crefydd, iechyd a geneteg unigolyn. Mae biometreg hefyd wedi’u cynnwys erbyn hyn os defnyddir y data hwnnw i adnabod unigolyn yn unigryw.

Nid ystyrir data sy’n ymwneud ag euogfarnau troseddol neu droseddau yn ddata categori arbennig, ond mae mesurau diogelwch ar wahân ar waith ar gyfer y math hwn o ddata yn Erthygl 10 o’r GDPR.

A fydd angen i mi gydymffurfio ag ef?

Nid ystyrir data sy’n ymwneud ag euogfarnau troseddol neu droseddau yn ddata categori arbennig, ond mae mesurau diogelwch ar wahân ar waith ar gyfer y math hwn o ddata yn Erthygl 10 o’r GDPR.

Does dim ots p’un a ydych chi wedi’ch lleoli o fewn un o aelod-wladwriaethau’r UE ai peidio: os yw eich mudiad yn prosesu data personol sy’n ymwneud â phreswylwyr yr UE, ac os ystyrir ei fod yn ‘rheolydd data’ neu’n ‘brosesydd data’, bydd gofyn i’ch mudiad gydymffurfio â’r GDPR.

Rheolydd data yw'r mudiad neu'r person (fel 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 fel rheoli'r gyflogres, dosbarthu post, systemau TG, a gwaredu gwastraff cyfrinachol.

Mae'r GDPR yn gosod rhwymedigaethau cyfreithiol penodol ar broseswyr data nad ydynt wedi bod ar waith o dan y Ddeddf Diogelu Data, a bydd atebolrwydd cyfreithiol ar broseswyr data nawr os ydynt yn gyfrifol am dor diogelwch data.

Sut mae'r GDPR yn wahanol i Ddeddf Diogelu Data 1998?

Er bod y DU yn parhau i ddilyn egwyddorion y GDPR drwy GDPR y DU, mae newidiadau'n cael eu gwneud o dan y Bil Data (Defnyddio a Mynediad). Nid yw'r rhan fwyaf o'r darpariaethau mewn grym eto (yn ystod diwedd 2025 a 2026). Mae'r Bil yn ceisio symleiddio cydymffurfiaeth i fudiadau a chynnal safonau uchel ar yr un pryd. Dylai mudiadau sicrhau bod ganddynt y wybodaeth ddiweddaraf gan y gallai diwygiadau effeithio ar rwymedigaethau ynghylch cydsyniad, cadw cofnodion ac asesiadau buddiannau cyfreithlon.

Mae llawer yn debyg rhwng y ddau ddarn o 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'u lleihau o 8 i 6, ond maent yn parhau i fod yn debyg iawn o ran cynnwys i'r 8 egwyddor a nodir yn y Ddeddf Diogelu Data.

Mae'r 6 egwyddor diogelu data a nodir yn y GDPR yn nodi y bydd data:

1. Yn cael ei brosesu'n gyfreithlon, yn deg ac mewn modd tryloyw mewn perthynas ag unigolion;
2. Yn cael ei gasglu at ddibenion penodedig, eglur a chyfreithlon, ac ni chaiff ei brosesu mewn unrhyw ffordd sy'n anghydnaws â'r dibenion hynny;
3. Yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y cânt eu prosesu ar eu cyfer;
4. Yn gywir a, lle y bo angen, yn cael ei gadw'n gyfredol;
5. Yn cael ei gadw mewn ffurf sy'n caniatáu nodi testunau data, am ddim mwy nag sy'n angenrheidiol at y dibenion y mae'r data personol yn cael ei brosesu ar eu cyfer;
6. Yn cael ei brosesu mewn modd sy'n sicrhau diogelwch priodol y data personol, gan ddefnyddio mesurau technegol neu sefydliadol priodol.

Mae'r GDPR hefyd yn nodi egwyddor atebolrwydd drosfwaol. Mae hyn yn ei gwneud yn ofynnol i reolwyr data fod yn gyfrifol am y 6 egwyddor a nodir uchod, a gallu dangos cydymffurfiaeth â nhw.

Hysbysiadau Preifatrwydd

Mae hysbysiad preifatrwydd yn ddatganiad rydych yn ei ddarparu i unigolion pan fyddwch yn casglu gwybodaeth ganddynt, ac mae'n nodi'r hyn sydd angen iddynt ei wybod ynghylch diogelu data. Mae'r GDPR yn cyflwyno gofyniad i ddarparu hysbysiadau preifatrwydd mwy manwl i unigolion pan gesglir data personol, gan gynnwys gwybodaeth fel:

- Y diben(ion) y bydd y data personol yn cael ei brosesu ar eu cyfer
- Y sail gyfreithiol y mae'r mudiad yn dibynnu arni i brosesu data'r unigolyn hwnnw (gweler isod)
- Am ba hyd y bydd y data yn cael ei gadw
- Gyda phwy y bydd neu y gall y data gael ei rannu, a
- Hawl yr unigolyn i dynnu cydsyniad yn ôl os yw'n dymuno gwneud hynny.

Ceir rhagor o fanylion am y wybodaeth y mae angen i chi ei darparu i unigolion ar wefan Swyddfa'r Comisiynydd Gwybodaeth.

Swyddogion Diogelu Data

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

- Rydych yn awdurdod cyhoeddus;
- Mae eich gweithgareddau craidd yn ei gwneud yn ofynnol i chi fonitro unigolion ar raddfa fawr, yn rheolaidd ac yn systematig (er enghraifft, olrhain ymddygiad ar-lein); neu
- Mae eich gweithgareddau craidd yn cynnwys prosesu categorïau arbennig o ddata neu ddata sy'n ymwneud ag euogfarnau troseddol a throseddau ar raddfa fawr.

Os nad ydych yn bodloni'r meini prawf hyn, gallwch benodi Swyddog Diogelu Data yn wirfoddol os dymunwch, ond dylech fod yn ymwybodol bod yr un gofynion yn berthnasol ar gyfer y swydd a'r tasgau ag y byddent pe bai'n orfodol i benodi'r Swyddog Diogelu Data.

Ceir gwybodaeth ychwanegol am y meini prawf a manylion rôl Swyddog Diogelu Data yng Nghanllaw Swyddfa'r Comisiynydd Gwybodaeth ar GDPR Canllaw Swyddfa'r Comisiynydd Gwybodaeth ar GDPR.

Fel arall, gallwch benodi rhywun i fod yn 'arweinydd' diogelu data eich mudiad (neu debyg), er mwyn iddo gydlynu darpariaethau diogelu data yn eich mudiad, ac o bosibl weithredu fel y person y mae staff a/neu wirfoddolwyr yn adrodd unrhyw doriadau diogelu data iddo, ond ni fydd yn rhaid iddo fodloni'r gofynion swyddogol sy'n gysylltiedig â rôl Swyddog Diogelu Data.

Ceir gwybodaeth ychwanegol am y meini prawf a manylion rôl Swyddog Diogelu Data yn y ddogfen Cwestiynau Cyffredin yn y ddolen isod.

Hawliau Ehangach

Mae'r Ddeddf Diogelu Data yn rhoi amrywiaeth o hawliau i unigolion mewn perthynas â'u data personol, ond bydd yr hawliau hynny'n cael eu hehangu gan y GDPR, a byddant yn cynnwys hawl newydd i

gludadwyedd data. Mae'r hawliau canlynol ar gyfer unigolion wedi'u nodi yn y GDPR:

- Yr hawl i gael gwybod
- Hawl mynediad
- Yr hawl i gywiro
- Yr hawl i ddileu (a elwir hefyd yn yr hawl i anghofio)
- Yr hawl i gyfyngu ar brosesu
- Yr hawl i gludadwyedd data
- Yr hawl i wrthwynebu
- Hawliau mewn perthynas â gwneud penderfyniadau awtomataidd a phroffilio

Lle mae mudiadau'n defnyddio deallusrwydd artiffisial (AI) i wneud penderfyniadau am unigolion (e.e. penderfyniadau sgrinio neu gymhwysedd awtomataidd), rhaid iddynt ystyried hawl yr unigolyn i beidio â bod yn destun penderfyniadau awtomataidd yn unig. Mae Swyddfa'r Comisiynydd Gwybodaeth yn argymell y dylid cynnal Asesiad o'r Effaith ar Ddiogelu Data (DPIA) a rhoi esboniadau clir i unigolion ynghylch sut mae systemau o'r fath yn gweithio.

Mae manylion llawn pob un o'r hawliau hynny i'w gweld ar wefan Swyddfa'r Comisiynydd Gwybodaeth.

Sail Gyfreithlon dros Brosesu Data

Cyn y gallwch chi brosesu unrhyw ddata personol, mae'r GDPR yn ei gwneud yn ofynnol i chi nodi sail gyfreithlon dros allu ei brosesu.

Mae 6 sail y gallwch ddewis dibynnu arnynt, a bydd angen i chi benderfynu pa un neu fwy ohonynt sy'n berthnasol i'ch gweithgareddau prosesu data.

Y 6 sail gyfreithlon sydd ar gael ar gyfer prosesu data yw:

Cydsyniad: mae'r unigolyn wedi rhoi cydsyniad clir i chi brosesu ei ddata personol at ddiben penodol (gweler isod am ragor o fanylion)

Contract: mae'r prosesu'n angenrheidiol ar gyfer contract sydd gennych gyda'r unigolyn, neu oherwydd ei fod wedi gofyn i chi gymryd camau penodol cyn ymrwymo i gontract.

Rhwymedigaeth gyfreithiol: mae'r prosesu'n angenrheidiol er mwyn i chi gydymffurfio â'r gyfraith (ond nid yw hyn yn cynnwys rhwymedigaethau cytundebol a allai fod gennych)

Buddiannau allweddol i fywyd: mae'r prosesu'n angenrheidiol i ddiogelu bywyd rhywun.

Tasg gyhoeddus: mae'r prosesu'n angenrheidiol er mwyn i chi gyflawni tasg er budd y cyhoedd neu ar gyfer eich swyddogaethau swyddogol, ac mae gan y dasg neu'r swyddogaeth sail glir yn y gyfraith (mae hyn yn fwyaf perthnasol i awdurdodau cyhoeddus, ond gall fod yn berthnasol i unrhyw fudiad sy'n arfer awdurdod swyddogol neu'n cyflawni tasgau er budd y cyhoedd)

Buddiannau dilys: mae'r prosesu'n angenrheidiol ar gyfer buddiannau dilys eich mudiad, neu fuddiannau dilys trydydd parti, oni bai bod rheswm da dros ddiogelu data personol yr unigolyn sy'n diystyru'r buddiannau dilys hynny.

Gall offeryn canllaw rhyngweithiol sail gyfreithlon Swyddfa'r Comisiynydd Gwybodaeth eich helpu gyda hyn.

Cydsyniad

O dan y Ddeddf Diogelu Data, os ydych yn dibynnu ar gydsyniad i brosesu data personol unigolyn, yn y rhan fwyaf o amgylchiadau gallwch naill ai ddibynnu ar gydsyniad penodol (lle mae'r unigolyn yn nodi ei fod yn iawn i chi ddefnyddio ei ddata mewn ffyrdd penodol), neu gydsyniad ymhlyg (lle nad yw'r unigolyn yn nodi nad yw am i chi ddefnyddio ei ddata).

Os ydych chi am ddibynnu ar gydsyniad fel y sail gyfreithlon i brosesu data personol unwaith y daw'r GDPR i rym, ni fyddwch yn gallu dibynnu ar gydsyniad ymhlyg mwyach. Bydd angen iddo fod yn gydsyniad 'optio i mewn' sy'n cael ei roi'n wirfoddol, yn benodol ac yn wybodus.

Mae hyn yn golygu bod y trothwy ar gyfer cydsyniad yn uwch o dan y GDPR, felly efallai y bydd angen i chi newid y ffordd rydych yn cael cydsyniad gan unigolion (os oes angen cydsyniad i chi brosesu eu data), a/neu efallai y bydd angen i chi gael cydsyniad newydd gan unigolion os nad ystyrir y bydd y cydsyniad sydd gennych eisoes yn cydymffurfio â'r GDPR.

Mae Swyddfa'r Comisiynydd Gwybodaeth wedi cyhoeddi canllawiau ar gydsyniad, sy'n cadarnhau'n union pa feini prawf sydd angen eu bodloni er mwyn i gydsyniad fod yn ddilys o dan y GDPR.

Noder, fodd bynnag, mai dim ond un o'r 6 opsiwn sydd gennych ar gyfer prosesu data personol yw cydsyniad, a gallai fod yn fwy priodol a/neu ymarferol i chi ddibynnu ar sail gyfreithlon wahanol i brosesu'r data yn lle hynny.

Rhoi Gwybod am Dor Diogelwch Data

O dan y Ddeddf Diogelu Data, nid oedd unrhyw rwymedigaeth gyfreithiol ar reolwyr data i roi gwybod am dor diogelwch data, ond mae'r GDPR yn cyflwyno dyletswydd ar bob mudiad i roi gwybod am achos o dor diogelwch data personol i Swyddfa'r Comisiynydd Gwybodaeth os ydynt yn credu ei bod yn debygol o

beryglu hawliau a rhyddid yr unigolyn/unigolion y mae'r achos o dor diogelwch data yn berthnasol iddynt.

Os yw'r mudiad yn credu bod risg o'r fath yn debygol, bydd angen iddo roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr i fod yn ymwybodol o'r tor diogelwch data (os yw'n bosibl gwneud hynny). Ac os yw'r tor diogelwch data yn debygol o arwain at risg uchel i hawliau a rhyddid yr unigolyn/unigolion y mae'r achos o dor diogelwch data yn berthnasol iddynt, bydd angen i'r mudiad hefyd roi gwybod i'r unigolion hynny am y tor diogelwch data heb oedi diangen.

O safbwynt ymarferol, mae hyn yn golygu bod angen i bob aelod o'ch staff a/neu bob gwirfoddolwr allu nodi achos o dor diogelwch data os bydd un yn digwydd, ac mae angen iddynt hefyd wybod i bwy y mae angen iddynt roi gwybod am dor diogelwch o'r fath ar unwaith, fel y gellir cyflwyno adroddiad i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr os oes angen. Gellir atal y rhan fwyaf o achosion o dor diogelwch data drwy gael mesurau diogelwch cadarn ar waith ym mhob rhan o'ch mudiad.

Dylai mudiadau ddogfennu pob achos o dor diogelwch data, ni waeth p'un a oes angen hysbysu Swyddfa'r Comisiynydd Gwybodaeth amdano ai peidio. Dylai hyd yn oed digwyddiadau risg isel (e.e. negeseuon e-bost a anfonir at y derbynnydd anghywir) gael eu cofnodi'n fewnol a'u hasesu.

Ceir rhagor o wybodaeth am achosion o dor diogelwch data a diogelwch ar wefan Swyddfa'r Comisiynydd Gwybodaeth.

Asesiadau o'r Effaith ar Ddiogelu Data

Ers peth amser, mae Swyddfa'r Comisiynydd Gwybodaeth wedi bod yn annog rheolwyr data i gynnal yr asesiadau hyn fel arfer da wrth weithio ar brosiectau sy'n cynnwys data personol. Yn ei hanfod, mae Asesiad o'r Effaith ar Ddiogelu Data yn broses i ddadansoddi'r ffordd rydych yn prosesu data, a'ch helpu i nodi a lleihau risgiau i ddiogelwch data. Bydd y GDPR yn ei gwneud yn orfodol i'r asesiadau hyn gael eu cynnal ar gyfer rhai ffyrdd o brosesu data, neu os yw prosesu data unigolyn yn debygol o arwain at risg uchel i fuddiannau'r unigolyn hwnnw.

Mae Swyddfa'r Comisiynydd Gwybodaeth wedi datgan bod hyn yn elfen allweddol o'r ffocws newydd sydd ar atebolrwydd a 'diogelu data drwy ddyluniad' o dan y GDPR, ynghyd â dull cydymffurfio sy'n fwy seiliedig ar risg.

Aeth Swyddfa'r Comisiynydd Gwybodaeth ati i ddiweddaru ei chanllawiau yn 2023, gan dynnu sylw at pryd mae Asesiad o'r Effaith ar Ddiogelu Data yn orfodol, megis ar gyfer monitro systematig, prosesu data categori arbennig ar raddfa fawr, neu ddefnyddio technoleg arloesol fel deallusrwydd artiffisial (AI). Rhaid i elusennau ystyried yr asesiadau hyn wrth gyflwyno llwyfannau newydd, offer codi arian, neu systemau dadansoddi data.

Ceir gwybodaeth fanwl am sut i gynnal Asesiad o'r Effaith ar Ddiogelu Data (os oes angen) yng Nghanllaw Swyddfa'r Comisiynydd Gwybodaeth ar y GDPR, ynghyd â nifer o restrau gwirio a allai fod yn ddefnyddiol i chi.

Dirwyon

O dan y Ddeddf Diogelu Data, mae gan Swyddfa'r Comisiynydd Gwybodaeth y p er i roi dirwyon o hyd at £500,000 am dor diogelwch data personol. Mae'r GDPR yn cyflwyno cynnydd yn lefel y dirwyon hynny, a gallai'r gosb uchaf fod hyd at £17.5m neu 4% o drosiant byd-eang (pa un bynnag sydd fwyaf).

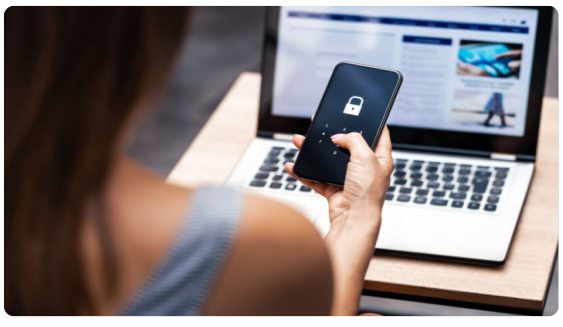
Fodd bynnag, mae Swyddfa'r Comisiynydd Gwybodaeth wedi cadarnhau mai dim ond pan fetho popeth arall y bydd yn rhoi dirwyon, fel y mae'n ei wneud nawr. Ynghyd â'r p er i roi dirwyon uwch os yw'n teimlo bod hynny'n angenrheidiol, bydd Swyddfa'r Comisiynydd Gwybodaeth yn parhau i allu rhoi cosbau eraill gan gynnwys rhybuddion, ceryddon a gorchmynion cywirol.

Beth alla i 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, gan gynnwys:
- Cynnal archwiliad i nodi pa ddata personol rydych yn ei ddal a'r hyn rydych yn ei wneud ag ef, ac yna cynnal asesiadau risg sy'n ymwneud â'r data hwnnw, yna rhoi mesurau ar waith i reoli unrhyw risgiau a nodwyd gennych. Mae gan Swyddfa'r Comisiynydd Gwybodaeth nifer o dempledi dogfennaeth a rhestrau gwirio a allai fod yn ddefnyddiol i chi, er enghraifft y rhestr wirio hunanasesu hon.
- Mae gan Swyddfa'r Comisiynydd Gwybodaeth nifer o dempledi dogfennaeth a rhestrau gwirio a allai fod yn ddefnyddiol i chi, er enghraifft y rhestr wirio hunanasesu hon.
- Os ydych yn dibynnu ar gydsyniad i brosesu data personol unrhyw unigolion, gwirio a yw'n bodloni'r trothwy uwch o dan y GDPR.
- Adolygu eich hysbysiadau preifatrwydd a sicrhau eu bod yn cynnwys y manylion ychwanegol y mae'r GDPR yn ei nodi sy'n ofynnol.
- Hyfforddi staff, gwirfoddolwyr a staff dros dro mewn diogelu data, a rhoi polisïau a gweithdrefnau ar waith ar draws eich mudiad i sicrhau bod data yn cael ei brosesu yn unol ag egwyddorion diogelu data.
- Penderfynu a oes angen i chi benodi Swyddog Diogelu Data.
- Sicrhau bod systemau ar waith i nodi achosion o dor diogelwch data ac adrodd amdanynt i Swyddfa'r Comisiynydd Gwybodaeth, yn ôl yr angen.

Am ganllawiau cyfredol ewch i: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Gwybodaeth Bellach



Pecyn Cymorth GDPR