Canllawiau Diogelu Data a Diogelwch Data i Gynhyrchwyr:
Criw Cynhyrchu – Nodiadau Cyffredinol

Mae'r nodiadau hyn yn cynnig cyngor a chymorth ymarferol i chi, ar gyfer trin **data personol pobl sy'n fyw (gan gynnwys data categori arbennig)** o dan Ddeddf Diogelu Data 2018, sy'n gweithredu'r Rheoliad Cyffredinol ar Ddiogelu Data (**GDPR**) a ddaeth i rym ar 25 Mai 2018.

Mae diogelu data unigolion yn fater pwysig. O dan y GDPR, gall cwmni cynhyrchu ddioddef sancsiynau troseddol a sifil os datgelir data personol neu ddata categori arbennig heb awdurdod, heb sôn am y difrod i enw da'r cwmni sy'n eich cyflogi, ac o bosib enw da'r darlledwr sydd wedi comisiynu'r gyfres briodol.

Ystyr data personol o dan y GDPR yw data sy'n ymwneud â bod dynol byw, y gellir ei adnabod o'r data hynny, neu o'r data hynny ynghyd ag unrhyw wybodaeth arall sydd ar gael yn hwylus e.e. **un neu ragor o'r canlynol:** enw'r unigolyn, ei gyfeiriad, rhifau teleffon, cyfeiriadau e-bost personol, dyddiad geni, manylion banc a chyflogres, perthynas agosaf, manylion pasbort, delweddau, cyfeiriad IP ac ati.

Mae data categori arbennig (a elwid gynt yn 'ddata personol sensitif') hefyd yn ddata personol ac yn wybodaeth y mae'n rhaid ei thrin â gofal ychwanegol. Mae'n cynnwys gwybodaeth am darddiad hiliol neu ethnig unigolyn, ei safbwyntiau gwleidyddol, credoau crefyddol, aelodaeth o undeb llafur, materion iechyd corfforol neu feddyliol, cyfeiriadedd rhywiol a data genetig a biometrig. Ni chaniateir ichi brosesu'r math hwn o ddata personol oni ellwch weithredu yn unol ag Erthygl 9 o'r GDPR[1], sy'n pennu'r amodau ychwanegol ar gyfer prosesu data categori arbennig. Os nad ydych yn sicr pa ddata categori arbennig y caniateir i chi eu prosesu, dylech ofyn i'ch rheolwr llinell. Sylwer: ar gyfer gwybodaeth am droseddau, a data plant, mae darpariaethau penodol wedi eu gwneud bellach, ar sut y dylid trin y mathau hyn o ddata. Dylech ofyn i'ch rheolwr llinell gadarnhau bod yr holl ragofalon angenrheidiol ar waith, ar gyfer trin data o'r mathau hyn. Os byddwch yn prosesu data personol plant dylech roi sylw o'r dechreuad i'r angen i'w hamddiffyn, a chynllunio eich systemau a'ch prosesau gyda hynny mewn golwg.

Er mwyn trin unrhyw fath o ddata personol o dan y GDPR, mae'n rhaid ichi gael **sail gyfreithlon**. Cyn casglu unrhyw ddata personol, mae'n bwysig eich bod yn deall, ac wedi cytuno gyda'ch cwmni cynhyrchu, ar ba sail gyfreithlon y byddwch yn prosesu data personol pan cewch eich cyflogi neu'ch contractio gan y cwmni; a bod y sail gyfreithlon honno wedi ei dogfennu. Er enghraifft, wrth ymdrin â chyfranwyr, bydd eich cytundeb gyda'r cyfranwyr yn datgan, yn ôl pob tebyg, mai sail gyfreithlon ar gyfer prosesu fydd naill ai 'ar gyfer cyflawni contract' neu 'buddiannau dilys'. Os na fydd eich rheolwr llinell wedi rhoi gwybod ichi, neu os byddwch yn ansicr ar ba sail gyfreithlon y byddwch yn dibynnu wrth gasglu neu drin data, dylech holi eich rheolwr llinell neu un o'r personél enwebedig.

Yma yn [*gosoder enw'r cwmni*], [*un o'r personél enwebedig*] sy'n gyfrifol o fewn y cwmni am gydymffurfio â'r GDPR. Dylech gysylltu â'r person hwnnw os ydych yn ansicr ynghylch eich rhwymedigaethau o dan y GDPR o ran casglu, defnyddio, prosesu, cyrchu neu ddinistrio data personol.

Casglu a chael mynediad i ddata personol

Byddwch yn cael mynediad at ac yn casglu data personol yn rheolaidd gan gynnwys, o bosib, data categori arbennig mewn sawl gwahanol ffurf. Mae'n bosib y daw'r wybodaeth gan gyflogeion, cyfranwyr, cyflenwyr neu gontractwyr, o'r gorffennol, y presennol a'r dyfodol.

Mae'n bosib fod yr wybodaeth fod ar ffurf llythyrau, negeseuon e-bost, gohebiaeth, cofnodion galwadau, triniaethau a threfnau rhaglenni, CVs, darnau ffilm cylch cyfyng, cytundebau, ffurflenni rhyddhau a ffurflenni cais cyfranwyr, taflenni galwadau, P-as-Cs, gwiriadau'r gwasanaeth datgelu a gwahardd *(DBS Checks)*, cofnodion

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

meddygol, anfonebau, archebion prynu, deunydd crai *(rushes)* â chapsiynau, cyfriflenni banc, rhestrau cyflogeion, geirdaon cyflogeion ac ati. Gall yr wybodaeth fod ar ffurf copïau caled, sef dogfennau papur gwreiddiol neu gopïau ohonynt, ffotograffau neu ffilm; neu ar ffurf electronig mewn cyfrifiaduron personol, gliniaduron, ffonau symudol neu BlackBerry, neu gofion bach.

Pa ddata personol y dylech chi eu casglu?

Dylech gasglu **dim mwy na'r hyn sydd ei angen arnoch. O dan y GDPR, hynny yw'r data personol sy'n angenrheidiol at y diben y byddwch yn eu defnyddio ar ei gyfer.** Er enghraifft, byddai'n rhesymol ichi gasglu enwau a manylion cyswllt cyfranwyr er mwyn trefnu i'w ffilmio; ond mae'n annhebygol iawn y byddai arnoch angen gwybodaeth am eu hanes rhywiol er mwyn cyflawni'r swyddogaeth honno, oni fydd yr hanes hwnnw'n berthnasol i'r rhaglen.

Beth y mae'n rhaid ichi ei ddweud wrth y person y gofynnwch am yr wybodaeth ganddo?

Dylech ddweud wrth y person hwnnw pam y mae angen ichi gasglu'r wybodaeth bersonol ac at ba ddiben y byddwch yn ei defnyddio, pa sail gyfreithlon a ddefnyddir gennych i brosesu'r wybodaeth bersonol, sut y caiff ei rhannu a'i storio, ac am ba hyd y cedwir yr wybodaeth; a dylech ei atgoffa bod ei hawliau mewn perthynas â data personol wedi'u diogelu gan y GDPR.

Pan gyflëir yr wybodaeth hon i'r unigolyn, dylid gwneud hynny yn *eglur a chryno* mewn iaith sy'n hawdd i'w deall. Os byddwch yn casglu data personol sy'n ymwneud â phlant, dylech sicrhau bod eich esboniad yn addas ar gyfer oedran y plentyn (oni fyddwch yn rhoi'r esboniad i'w riant/gwarcheidwad), fel y gall y plentyn ddeall beth fydd yn digwydd i'w ddata ac ystyried a ddylech chi gysylltu hefyd â'i riant neu'i warcheidwad.

Sut y cewch ddefnyddio'r wybodaeth?

Cewch ddefnyddio data personol at y dibenion hynny y casglwyd y data gennych neu y'u rhoddwyd ichi ar eu cyfer yn unig. Er enghraifft, mae'n bosibl y rhoddwyd y data personol gan gyfrannwr at ddibenion rhaglen benodol yn unig, ac nid at unrhyw ddiben arall. Fodd bynnag, os byddwch, er enghraifft, yn dymuno cysylltu eto â'r rhai a wnaeth gais i gymryd rhan mewn rhaglen, ynglŷn â chymryd rhan mewn rhaglenni eraill yn y dyfodol, neu ynglŷn â chael gwybodaeth farchnata, cewch ofyn iddynt gydsynio i hynny. Rhaid i gydsyniad o'r fath gael ei roi yn rhydd a phenodol, a rhaid i'r unigolyn optio i mewn i bob diben unigol (dylech ddynodi hefyd sut y gall yr unigolyn dynnu ei gydsyniad yn ôl). Os byddwch yn defnyddio cydsyniad o'r fath, cofiwch na ellir gwneud cydsynio yn amod cynnwys yr unigolyn mewn rhaglen, ac y dylech roi gwybod i'r unigolyn y caiff dynnu ei gydsyniad yn ôl, a sut y gall gwneud hynny. Dylid datgan hyn yn benodol ar unrhyw ffurflen a ddefnyddir gennych.

Sicrhau bod data yn ddienw

Gellir defnyddio dull effeithiol o sicrhau bod data yn ddienw er mwyn cyhoeddi data a fyddai, fel arall, yn ddata personol. Mae Swyddfa'r Comisiynydd Gwybodaeth yn diffinio'n broses o sicrhau bod data yn ddienw fel y broses o roi data mewn ffurf nad yw'n caniatáu i unigolion gael eu hadnabod, ac nad yw adnabyddiaeth o'r fath yn debygol o ddigwydd trwy gyfuno'r data gyda data eraill. Dylid cwblhau asesiad risg cyn prosesu'r cyfryw ddata dienw. Prawf buddiol y gellid ei ddefnyddio ar gyfer hynny yw'r Prawf Ymyrrwr Ewyllysgar *(Motivated Intruder Test)*.

Gellid defnyddio dulliau di-enw yn effeithiol er mwyn galluogi aelodau o gynulleidfa rannu straeon a phrofiadau pan fo'r data y maent am ei rannu yn sensitif. Er enghraifft, pe byddai unigolion yn dymuno cyfrannu at stori am eu profiadau gyda'r GIG, hwyrach y byddai angen cydgrynhoi'r cyfraniadau hynny neu sicrhau eu bod yn ddienw, a hynny er mwyn ategu at y stori heb ei chysylltu ag unigolyn penodol. Gellid hefyd ddefnyddio dulliau i sicrhau bod data yn ddienw pan fo sefydliad yn dymuno rhannu data at ddibenion ymchwil.

http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

Trin data personol

1. Dylid cadw data personol yn ddiogel, rhag eu colli neu'u difrodi a rhag mynediad diawdurdod. Dylech sicrhau na chaiff data personol eu gadael ar eich desg pan na fyddwch yn bresennol. Dylid cadw data o'r fath o dan glo mewn swyddfa neu fan diogel arall. Pan fo'n briodol, dylid cadw ffeiliau sy'n cynnwys Data Categori Arbennig dan glo neu i ffwrdd o'r safle. Os na fyddwch yn sicr pa drefniadau diogelwch sy'n bodoli, dylech holi uwch-aelod o'r staff neu un o'r personél enwebedig.

2. A ydych wedi diogelu eich cyfrifiadur gyda chyfrinair, ac a fyddwch yn diweddaru'r cyfrinair hwnnw yn rheolaidd? Os byddwch yn defnyddio neu'n cael mynediad at ddata personol a allai achosi niwed pe caent eu dwyn, eu colli neu'u datgelu yn amhriodol (er enghraifft, cofnodion ariannol, gwybodaeth iechyd, data am blant neu ddata categori arbennig eraill), dylai'ch cyfrifiadur, gliniadur neu ddyfeisiau eraill fod wedi eu diogelu â chyfrinair, a'ch bwrdd gwaith gyda wal dân ddiogel.

3. A ydych yn darparu neu'n cyfyngu ar fynediad i wybodaeth, boed ar gyfrifiaduron neu mewn copïau caled, i'r unigolion hynny yn unig sydd wedi'u hawdurdodi, neu sydd arnynt angen cael mynediad? Rhaid ichi sicrhau *bod unrhyw ddogfen sy'n cynnwys data personol (sef pob dogfen o'r bron!) wedi ei storio yn electronig naill ai (a) mewn rhan ddiogel o'r gweinydd sydd â chyfyngiadau mynediad priodol neu (b) mewn ffolder wedi ei amgryptio neu'i amddiffyn â chyfrinair.*

4. Byddwch yn ofalus wrth agor negeseuon e-bost anghyfarwydd ac atodiadau neu wrth ymweld â gwefannau, i rwystro feirysau rhag peryglu diogelwch eich data.

5. Dylech leoli eich sgriniau cyfrifiadur, hysbysfyrddau a byrddau gwyn yn ddigon pell oddi wrth ffenestri, neu o olwg y cyhoedd, rhag datgelu data personol yn ddamweiniol.

6. Sicrhewch na all gwesteion neu ymwelwyr â'ch swyddfa weld unrhyw ddata personol, a chymerwch gamau priodol rhag datgelu data o'r fath iddynt yn ddamweiniol.

7. A oes caniatâd gennych i fynd â chyfrifiaduron, gliniaduron, disgiau cyfrifiadurol ac ati i ffwrdd o'r safle? Os oes, gwiriwch fod ynddynt ddiogelwch cyfrinair priodol; ac ar gyfer data personol, data categori arbennig, data troseddol, data plant a data ariannol, gwiriwch fod lefel uchel o amgryptio yn y ffolderi perthnasol neu yn y cyfrifiadur/disgiau cyfan, neu fath arall o ddiogelwch effeithiol. Os oes gennych ffôn symudol gwaith sy'n cynnwys manylion cyfranwyr ac ati, dylech ei gadw wedi ei gloi â chyfrinair a'i godio; pe bai'r cyfarpar wedyn cael ei ddwyn neu'u golli, neu rywun yn ceisio hacio i mewn iddo, byddai'r data personol yn ddiogel. Os collir dyfeisiau cludadwy/ symudol, sy'n cynnwys cyfryngau magnetig a ddefnyddir i storio a thrawsyrru data personol, gall hynny achosi niwed/trallod difrifol i'r unigolyn trwy ddatgelu'r data i'r cyhoedd. Mewn cyfarpar o'r fath, mae Swyddfa'r Comisiynydd Gwybodaeth yn argymell defnyddio meddalwedd amgryptio cymeradwy, a ddyfeisiwyd i rwystro camddefnyddio'r wybodaeth.

8. Dylech roi gwybod i'ch rheolwr llinell pan fyddwch yn symud data personol o'r safle, a hefyd wrth ddychwelyd y data i'r safle.

9. Peidiwch â gwneud mwy na'r union nifer o gopïau o ddata personol ar gyfer eu dosbarthu i bobl sydd arnynt eu hangen (a hynny eto yn unig at y dibenion y casglwyd y data ar eu cyfer); a sicrhewch fod y derbynwyr yn gwybod bod angen, ac yn gallu, diogelu'r wybodaeth yn y modd a bennir yn y canllawiau hyn.

10. Sicrhewch eich bod yn gwybod pa ddogfennau y dylid eu rhwygo a/neu'u rhoi yn y biniau/blychau ailgylchu "diogel".

11. Byddwch yn arbennig o ofalus wrth ffacsio/ anfon data personol, a sicrhau mai'r derbynnydd a fwriedir, yn unig, a fydd yn cael yr wybodaeth. Dylech ddefnyddio'r dull mwyaf diogel sydd ar gael bob amser wrth rannu gwybodaeth.

12. Os byddwch yn cael cais am wybodaeth gan yr heddlu dylech roi gwybod i'ch rheolwr llinell **ar unwaith** a phan fo'n briodol gofynnwch am gyngor yn ddi-oed gan y darlledwr sydd wedi comisiynu'r rhaglen briodol. Os yw'r cais yn ymwneud â deunydd rhaglen, gan gynnwys deunydd crai (*rushes*), dylech ymgynghori â'r darlledwr cyn gwneud unrhyw ddatgeliad, oherwydd gall fod seiliau cyfreithiol a golygyddol dilys dros wrthwynebu datgelu.

13. Pan ddaw gwaith cynhyrchu i ben, dylech sicrhau bod uwch-aelod o'r staff yn adolygu pa gofnodion data personol y gellir yn gyfreithlon eu cadw neu'u dinistrio. Dichon y bydd angen dilys i'r cwmni cynhyrchu gadw rhywfaint o wybodaeth at ddibenion cyfreithiol neu ddibenion busnes; er enghraifft, pe bai damwain wedi digwydd, neu achos llys ar droed, byddai'n rhaid cadw rhai dogfennau am resymau cyfreithiol. Dylech sicrhau bod gennych y caniatâd mewnol angenrheidiol ar gyfer dinistrio data personol.

14. A ydych yn sicr eich bod wedi dychwelyd a/neu ddinistrio unrhyw ddogfennau, cofion bach, DVDs ac ati a symudwyd gennych o'r safle? Os bydd angen i chi ddinistrio dogfennau, a ydych wedi cael caniatâd perthnasol gan eich rheolwr llinell?

15. Ar ddiwedd eich cyflogaeth gyda'r cwmni, a ddychweloch chi'r holl ddata cyfrinachol neu bersonol , neu (os cytunodd y cwmni ichi wneud hynny) a ddileoch chi'r wybodaeth gyfrinachol neu bersonol o unrhyw gyfrifiaduron personol neu ddyfeisiau symudol a ddefnyddid gennych?

Toriad Diogelwch

Os daw toriad diogelwch i'ch sylw, neu ddatgeliad diawdurdod, neu golled/lladrad dogfennau neu wybodaeth mewn ffurf arall, rhaid ichi roi gwybod ar unwaith i'ch rheolwr llinell ac i'r uwch-aelod o'r staff sy'n gyfrifol am faterion diogelu data. Mae hyn yn ofynnol oherwydd y terfynau amser y mae'r GDPR yn eu gosod ar gwmnïau ar gyfer adrodd wrth Swyddfa'r Comisiynydd Gwybodaeth am doriadau diogelwch. Golyga hyn, er enghraifft, y byddai'n rhaid i gwmni cynhyrchu (yn dibynnu ar y math o doriad) adrodd wrth Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr wedi i'r toriad ddod i sylw'r cwmni. Pan fo'r toriad yn ymwneud â deunydd rhaglen (er enghraifft, yn ymwneud â chyfranwyr, cystadleuwyr neu dalent), dylai'ch rheolwr llinell, cyn gynted ag y daw i wybod am y toriad, hysbysu'r darlledwr sydd wedi comisiynu'r rhaglen berthnasol a chymryd pa bynnag gamau eraill a fyddai'n fuddiol.

Canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar adrodd am doriadau - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Dylech weithredu ar unwaith hefyd i ganfod maint y niwed posibl i'r unigolyn/unigolion perthnasol, a chymryd camau ar unwaith i liniaru unrhyw niwed neu ddifrod iddynt. Fodd bynnag, peidiwch â chysylltu ag unrhyw unigolyn hyd nes cyfarwyddir chi i wneud hynny. Bydd eich rheolwr llinell neu'r aelod enwebedig o'r personél yn cytuno ar y ffordd orau i weithredu o ran rhoi gwybod i unigolion, a phan fo'n briodol, i'r awdurdod rheoleiddiol perthnasol megis Swyddfa'r Comisiynydd Gwybodaeth.

Dylech wybod [Os gwelwch yn dda, mewnosodwch yma wybodaeth berthnasol am bolisïau eich cwmni chi, neu'r cyngor a chymorth ymarferol sydd ar gael gan eich cwmni cynhyrchu i ofalu bod data personol yn cael eu trin yn ddiogel, er enghraifft: lleoliad peiriannau rhwygo, biniau ailgylchu "diogel", cypyrddau cloadwy, deunydd wrth gefn cyfrifiadurol awtomatig, y ddarpariaeth o gyfarpar a ddiogelir gan gyfrineiriau neu rywfodd arall, cymorth TG ynghyd â dolenni cyswllt â pholisïau perthnasol eraill y cwmni, er enghraifft ar ddefnyddio'r Rhyngrwyd ac e-bost].

Cofiwch: Rhaid diogelu a pharchu data personol. Peidiwch â cholli data personol, na chaniatáu i neb eu dwyn. Dylech eu trin fel eich data (neu'ch arian) chi eich hun.

DIWEDD