POLISI DIOGELU DATA ANTHEM

Cofnod Hanes Newidiadau

Cyhoeddiad	Disgrifiad o’r Newid	Cymeradwywyd	Dyddiad Cyhoeddi
	Cyhoeddiad cychwynnol	Rhian Hutchings	27.01.2021
	Adolygiad diwethaf	Bwrdd o Anthem	July 2026

1. Cyflwyniad

1.1 Cefndir i Ddiogelu Data a GDPR y DU.

Mae Deddf Diogelu Data 2018 yn nodi’r fframwaith ar gyfer cyfraith diogelu data yn y DU. Mae’n diweddaru a disodli Deddf Diogelu Data 1998 a daeth i rym ar 25 Mai 2018. Fe’i diwygiwyd ar 01 Ionawr 2021 gan reoliadau o dan Ddeddf yr Undeb Ewropeaidd (Ymadael) 2018, i adlewyrchu statws y DU y tu allan i’r UE.

Mae’n cyd-sefyll â GDPR y DU ac yn ychwanegu ato – er enghraifft drwy ddarparu eithriadau. Y mae hefyd yn nodi rheolau diogelu data ar wahân i awdurdodau gorfodi’r gyfraith, yn ymestyn mesurau diogelu data i rai meysydd eraill megis diogelwch cenedlaethol ac amddiffyn, ac yn nodi swyddogaethau a phwerau’r Comisiynydd Gwybodaeth.

GDPR y DU yw Rheoliad Cyffredinol ar Ddiogelu Data y DU. Deddf y DU ydyw a ddaeth i rym ar 01 Ionawr 2021. Mae’n nodi egwyddorion, hawliau a rhwymedigaethau allweddol ar gyfer y rhan fwyaf o brosesu data personol yn y DU, ar wahân i asiantaethau gorfodi’r gyfraith ac asiantaethau cudd-wybodaeth. Mae’n seiliedig ar GDPR yr UE (Y Rheoliad Cyffredinol ar Ddiogelu Data (UE) 2016/679) a oedd yn berthnasol yn y DU cyn y dyddiad hwnnw, gyda rhai newidiadau fel ei fod yn gweithio’n fwy effeithiol yng nghyd-destun y DU.

1.2 Diffiniadau a ddefnyddir gan y sefydliad (a ddaw o’r GDPR)

Cwmpas ymarferol (Erthygl 2) – Mae GDPR y DU yn berthnasol i brosesu data personol yn llwyr neu’n rhannol gan ddulliau awtomatig (h.y. gan gyfrifiadur) ac i brosesu data personol ar wahân i gan ddulliau awtomatig (h.y. cofnodion papur) sy’n ffurfio rhan o system ffeilio neu y bwriedir iddynt ffurfio rhan o system ffeilio.

Cwmpas tiriogaethol (Erthygl 3) – Bydd GDPR y DU yn berthnasol i bob rheolydd sy’n sefydledig yn y DU neu sy’n prosesu data personol testun data, yng nghyd-destun y sefydliad

hwnnw. Bydd hefyd yn berthnasol i reolyddion y tu allan i'r DU sy'n prosesu data personol er mwyn cynnig nwyddau a gwasanaethau neu fonitro ymddygiad testunau data sy'n preswylio yn y DU.

1.3 Diffiniadau Erthygl 4

Sefydliad **–** prif sefydliad y rheolydd yn y DU fydd y lle y mae'r rheolydd yn gwneud y prif benderfyniadau ynglŷn â diben a dulliau ei weithgareddau prosesu data. Prif sefydliad prosesydd yn y DU fydd ei ganolfan weinyddol.

Data personol – unrhyw wybodaeth sy'n ymwneud â bod dynol ('testun data') adnabyddedig neu adnabyddadwy; mae bod dynol adnabyddadwy yn rhywun y gellir ei adnabod, yn uniongyrchol neu'n anuniongyrchol, yn benodol drwy gyfeiriad at ddyfais adnabod megis enw, rhif adnabod, data lleoliad, dyfais adnabod ar-lein neu at un neu ragor o ffactorau sy'n benodol i adnabyddiaeth gorfforol, ffisiolegol, genetig, meddyliol, economaidd, diwylliannol neu gymdeithasol y bod dynol hwnnw.

Categorïau arbennig o ddata personol – data personol sy'n datgelu tarddiad hil neu ethnig, barnau gwleidyddol, credoau crefyddol neu athronyddol, neu aelodau o undeb llafur, a phrosesu data genetig, data biometrig at ddiben adnabod bod dynol yn unigryw, data yn ymwneud ag iechyd neu ddata yn ymwneud â bywyd rhywiol neu gyfeiriadedd rhywiol bod dynol.

Rheolydd data – y bod dynol neu gyfreithiol, awdurdod cyhoeddus, asiantaeth neu gorff arall sydd, ar ei ben ei hun neu ar y cyd ag eraill, yn penderfynu ar ddibenion a dulliau prosesu data personol; lle y caiff dibenion a dulliau prosesu o'r fath eu pennu gan gyfraith y DU, gallai'r rheolydd neu'r meini prawf penodol ar gyfer enwebu rheolydd gael eu darparu ar eu cyfer gan gyfraith y DU.

Testun data – unrhyw unigolyn byw sy'n destun data personol a ddelir gan sefydliad.

Plentyn **–** mae'r GDPR yn diffinio plentyn fel unrhyw un o dan 16 mlwydd oed. Mae prosesu data personol plentyn yn gyfreithlon yn unig os yw cydsyniad rhiant neu geidwad wedi'i gael. Bydd y rheolydd yn gwneud ymdrechion rhesymol mewn achosion o'r fath i wirio bod cydsyniad wedi'i roi neu'i awdurdodi gan ddeiliad cyfrifoldeb rhieni dros y plentyn.

Cydsyniad testun data **–** mae hyn yn golygu unrhyw fynegiant penodol, diamwys wedi'i roi'n rhydd ac ar sail gwybodaeth o ddymuniadau testun y data y mae ef, hi neu hwy, drwy ddatganiad neu drwy weithred gadarnhaol glir, yn dynodi cytundeb i brosesu data personol.

Prosesu – unrhyw weithrediad neu set o weithrediadau a gynhelir ar ddata personol neu ar setiau o ddata personol, boed drwy ddulliau awtomatig neu beidio, megis casglu, cofnodi, trefnu, strwythuro, storio, addasu neu newid, adalw, ymgynghori, defnyddio, datgelu drwy drosglwyddiad, lledaenu neu wneud ar gael fel arall, alinio neu gyfuno, cyfyngu, dileu neu ddinistrio.

Proffilio – unrhyw ffurf ar brosesu data personol yn awtomatig sydd â'r bwriad o werthuso agweddau personol penodol yn ymwneud â bod dynol, neu ddadansoddi neu ragweld perfformiad y person hwnnw yn y gwaith, ei sefyllfa economaidd, lleoliad, iechyd, dewisiadau personol, dibynadwyedd, neu ymddygiad. Mae'r diffiniad hwn yn gysylltiedig â hawl testun data i wrthwynebu i broffilio a hawl i gael gwybod am bresenoldeb proffilio, mesurau'n seiliedig ar broffilio ac effeithiau proffilio a ragwelir ar yr unigolyn.

Tor diogelwch data personol – tor diogelwch sy'n arwain at, yn ddamweiniol neu'n anghyfreithlon, ddinistrio, colli, newid, datgelu neu fynediad heb ei awdurdodi at ddata personol sydd wedi'i drosglwyddo, storio neu'i brosesu fel arall. Mae rhwymedigaeth ar y rheolydd i adrodd achosion o dor diogelwch data personol i'r awdurdod goruchwylio, a lle y bo'n debygol bod yr achos o dor diogelwch am effeithio'n andwyol ar ddata personol neu breifatrwydd testun y data.

Trydydd parti – bod dynol neu gyfreithiol, awdurdod cyhoeddus, asiantaeth neu gorff arall ar wahân i destun y data, rheolydd, prosesydd a phersonau sydd, o dan awdurdod uniongyrchol y rheolydd neu'r prosesydd, wedi'i awdurdodi i brosesu data personol.

System ffeilio – unrhyw set strwythuredig o ddata personol sy'n hygyrch yn ôl meini prawf penodol, boed yn ganolog, datganoledig neu wasgaredig ar sail swyddogaethol neu ddaearyddol.

Staff – unrhyw un sy'n gweithio i Anthem neu gydag Anthem ar sail barhaol, dros dro, llawrydd, gwirfoddol neu gontractiol, gan gynnwys Cyfarwyddwyr.

2. Datganiad polisi

2.1 Mae Bwrdd Cyfarwyddwyr a rheolwyr Anthem, wedi'u lleoli ym Temple of Peace, King Edward VII Ave, Cardiff CF10 3AP, wedi ymrwymo i gydymffurfio â holl ddeddfau perthnasol y DU mewn perthynas â data personol, a diogelu "hawliau a rhyddid" unigolion y mae Anthem yn casglu a phrosesu eu gwybodaeth yn unol â Rheoliad Cyffredinol ar Ddiogelu Data y DU (GDPR y DU).

2.2 Mae cydymffurfiaeth â GDPR y DU yn cael ei ddisgrifio gan y polisi hwn a pholisïau perthnasol eraill, ynghyd â phrosesau a gweithdrefnau cysylltiedig.

2.3 Mae GDPR y DU a'r polisi hwn yn berthnasol i holl swyddogaethau prosesu data personol Anthem, gan gynnwys y rhai a gynhelir ar ddata personol cwsmeriaid, cleientiaid, cyflogeion, cyflenwyr a phartneriaid, ac unrhyw ddata personol arall o unrhyw ffynhonnell y mae'r sefydliad yn ei brosesu.

2.4 Y Swyddog Diogelu Data (SDD) sy'n gyfrifol am adolygu'r gofrestr brosesu yn flynyddol yng ngoleuni unrhyw newidiadau i weithgareddau Anthem (fel a bennir gan newidiadau i'r gofrestr asedau gwybodaeth a'r adolygiad rheoli) ac i unrhyw ofynion ychwanegol a nodir yn sgil asesiadau o'r effaith ar ddiogelu data. Mae angen i'r gofrestr hon fod ar gael ar gais yr awdurdod goruchwylio.

2.5 Mae'r polisi hwn yn berthnasol i holl Staff Anthem a phartïon a chanddynt fuddiant. Ymdrinnir ag unrhyw achos o fynd yn groes i GDPR y DU o dan bolisi disgyblu Anthem a gallai hefyd fod yn drosedd, ac os felly caiff y mater ei adrodd cyn gynted â phosibl i'r awdurdodau priodol.

2.6 Bydd disgwyl i bartneriaid ac unrhyw drydydd partïon sy'n gweithio gydag Anthem neu i Anthem, ac sydd â mynediad neu a allai fod â mynediad i ddata personol, fod wedi darllen a deall y polisi hwn a chydymffurfio ag ef. Ni chaiff unrhyw drydydd parti fynediad at ddata personol y mae Anthem yn ei ddal heb yn gyntaf ddod i gytundeb cyfrinachedd data gan ddilyn canllawiau'r SDD, sy'n gosod rhwymedigaethau ar y trydydd parti nad ydynt yn llai beichus na'r hyn y mae Anthem wedi ymrwymo iddynt, ac sy'n rhoi i Anthem yr hawl i archwilio cydymffurfiaeth â'r cytundeb.

3. Cyfrifoldebau a rolau o dan y Rheoliad Cyffredinol ar Ddiogelu Data

3.1 Mae Anthem yn rheolydd data ac yn brosesydd data o dan GDPR y DU.

3.2 Mae'r Prif Swyddog Gweithredol a phawb sydd mewn rolau rheoli neu oruchwylio ar draws Anthem yn gyfrifol am ddatblygu ac annog arferion trin gwybodaeth da oddi mewn i Anthem; mae'r cyfrifoldebau wedi'u nodi mewn swydd-ddisgrifiadau unigol.

3.3 Y Swyddog Diogelu Data (SDD) (Swydd-ddisgrifiad Swyddog Diogelu Data (SDD) Data a Chyfrifoldebau Swydd-ddisgrifiad Diogelu Data), rôl sydd wedi'i nodi yn GDPR y DU, ac mae'n atebol i Fwrdd Cyfarwyddwyr Anthem am reoli data personol oddi mewn i Anthem ac am sicrhau bod modd dangos cydymffurfiaeth â deddfwriaeth diogelu data ac ymarfer da. Mae'r atebolrwydd hwn yn cynnwys:

3.3.1 datblygu a gweithredu GDPR y DU fel sy'n ofynnol gan y polisi hwn;

3.3.2 diogelwch a rheoli risg mewn perthynas â chydymffurfiaeth â'r polisi.

3.4 Mae'r Swyddog Diogelu Data (SDD), y mae Bwrdd y Cyfarwyddwyr yn ystyried yn addas o gymwys a phrofiadol, wedi'u penodi i gymryd cyfrifoldeb am gydymffurfiaeth Anthem â'r polisi hwn o ddydd i ddydd ac, yn benodol, mae ganddynt gyfrifoldeb uniongyrchol am sicrhau bod Anthem yn cydymffurfio â GDPR y DU.

3.5 Mae gan y Swyddog Diogelu Data (SDD) gyfrifoldebau penodol mewn perthynas â gweithdrefnau'n ymwneud â diogelu data a hwy yw'r pwynt cyswllt cyntaf i Staff sydd eisiau eglurhad ar unrhyw agwedd ar gydymffurfio â diogelu data.

3.6 Mae cydymffurfio â deddfwriaeth diogelu data yn gyfrifoldeb ar holl Staff Anthem sy'n prosesu data personol.

3.7 Mae cynllun Cynefino Staff Anthem yn nodi gofynion penodol mewn perthynas â rolau penodol a Staff Anthem yn gyffredinol yn ymwneud â chydymffurfio â holl bolisïau a gweithdrefnau'r sefydliad sy'n gysylltiedig â GDPR y DU.

3.8 Mae Staff Anthem yn gyfrifol am sicrhau bod unrhyw ddata personol amdanynt hwy ac a gyflenwyd i Anthem yn gywir ac wedi'i ddiweddaru.

4. Egwyddorion diogelu data

Rhaid i unrhyw gamau prosesu data gael eu cynnal yn unol â'r egwyddorion diogelu data fel sydd wedi'u nodi yn Erthygl 5 GDPR y DU. Mae polisïau a gweithdrefnau Anthem wedi'u dylunio i sicrhau cydymffurfiaeth â'r egwyddorion.

4.1 <u>Rhaid i ddata personol gael ei brosesu'n gyfreithlon, teg a thryloyw</u>
Yn gyfreithlon – nodwch sail gyfreithlon cyn i chi allu prosesu data personol. Cyfeirir at y rhain yn aml fel "amodau ar gyfer prosesu"; cydsyniad, er enghraifft.

Yn deg – er mwyn i brosesu fod yn deg, rhaid i'r rheolydd data sicrhau bod gwybodaeth benodol ar gael i destunau'r data fel sy'n ymarferol. Mae hyn yn berthnasol p'un a gafwyd y data personol yn uniongyrchol oddi wrth destunau'r data neu o ffynonellau eraill.

Yn dryloyw – Mae GDPR y DU yn cynnwys rheolau ar roi gwybodaeth am breifatrwydd i destunau data yn Erthyglau 12, 13 a 14. Mae'r rhain yn fanwl a phenodol, ac yn rhoi pwyslais ar sicrhau bod hysbysiadau preifatrwydd yn ddealladwy a hygyrch. Rhaid i'r wybodaeth gael ei chyfathrebu i destun y data mewn ffurf ddealladwy gan ddefnyddio iaith glir a phlaen.
Mae Hysbysiad Preifatrwydd Anthem ar gael yn gyhoeddus fan yma ac mae ar gael i'r holl aelodau staff ar Google Drive y sefydliad.

Rhaid i'r wybodaeth bersonol y mae'n rhaid ei darparu i destun y data, yn y man lleiaf, gynnwys:

4.1.1 adnabyddiaeth a manylion cyswllt y rheolydd ac, os oes, cynrychiolydd y rheolydd;
4.1.2 manylion cyswllt y Swyddog Diogelu Data (SDD);
4.1.3 at ba ddibenion prosesu y bwriedir y data personol yn ogystal â'r sail gyfreithiol i'r prosesu;
4.1.4 am ba gyfnod y caiff y data personol ei storio;
4.1.5 bodolaeth yr hawliau i ofyn am fynediad, cywiro, dileu neu wrthwynebu i'r prosesu, a'r amodau (neu ddiffyg amodau) yn ymwneud ag arfer yr hawliau yma, megis a fydd cyfreithlondeb camau prosesu blaenorol yn cael ei effeithio;
4.1.6 categorïau'r data personol dan sylw;
4.1.7 derbynwyr neu gategorïau derbynwyr y data personol, lle y bo'n berthnasol;
4.1.8 lle y bo'n berthnasol, bod y rheolydd yn bwriadu trosglwyddo data personol i dderbynnydd mewn trydedd wlad a'r lefel o ddiogelwch a roddir i'r data;
4.1.9 unrhyw wybodaeth bellach sy'n angenrheidiol i warantu bod y prosesu'n deg.

4.2 Gall data personol gael ei storio at ddibenion penodol, eglur a dilys yn unig

Ni cheir defnyddio data a gafwyd at ddibenion penodol at ddiben sy'n wahanol i'r hyn a hysbyswyd yn ffurfiol i'r awdurdod goruchwylio fel rhan o gofrestr brosesu GDPR y DU Anthem. Mae'r Hysbysiad Preifatrwydd yn nodi'r gweithdrefnau perthnasol.

4.3 Rhaid i ddata personol fod yn ddigonol, perthnasol a chyfyngedig i'r hyn sy'n angenrheidiol i'w brosesu

4.3.1 Mae'r Swyddog Diogelu Data (SDD) yn gyfrifol am sicrhau nad yw Anthem yn casglu gwybodaeth nad yw'n gwbl angenrheidiol at y diben y mae wedi'i chael.
4.3.2 Rhaid i bob ffurflen casglu data (electronig neu bapur), gan gynnwys gofynion casglu data mewn systemau gwybodaeth newydd, gynnwys datganiad prosesu teg neu ddolen i ddatganiad preifatrwydd a'i gymeradwyo gan y Swyddog Diogelu Data (SDD)
4.3.3 Bydd y Swyddog Diogelu Data (SDD) yn sicrhau y caiff yr holl ddulliau casglu data eu hadolygu gan archwiliad mewnol i sicrhau bod y data a gesglir yn parhau i fod yn ddigonol a pherthnasol a heb fod yn ormodol.

4.4 Rhaid i ddata personol fod yn gywir a'i gadw wedi'i ddiweddaru gan wneud pob ymdrech i ddileu neu gywiro yn ddiymdroi

4.4.1 Rhaid i ddata sy'n cael ei storio gan y rheolydd gael ei adolygu a'i ddiweddaru yn ôl yr angen. Ni ddylid cadw unrhyw ddata oni bai ei fod yn rhesymol tybio ei fod yn gywir.

4.4.2 Mae'r Swyddog Diogelu Data yn gyfrifol am sicrhau bod yr holl staff wedi'u hyfforddi ym mhwysigrwydd casglu data cywir a'i gynnal.

4.4.3 Cyfrifoldeb testun y data hefyd yw sicrhau bod data sy'n cael ei ddal gan Anthem yn gywir ac wedi'i ddiweddaru. Pan fydd testun data yn llenwi ffurflen gofrestru neu ffurflen gais, bydd yn cynnwys datganid bod y data sydd wedi'i gynnwys yn y ffurflen yn gywir ar ddyddiad ei chyflwyno.

4.4.4 Dylai fod yn ofynnol i Staff a phartïon a chanddynt fuddiant, megis cyfranogwyr mewn prosiectau ac aelodau cynulleidfa, hysbysu Anthem o unrhyw newidiadau i'w hamgylchiadau i alluogi i gofnodion personol gael eu diweddaru yn unol â hynny. Mae cyfarwyddiadau i ddiweddaru cofnodion wedi'u cynnwys yn yr hysbysiad preifatrwydd (ar gael yn gyhoeddus) a'r polisi Dargadw Data (at ddefnydd mewnol). Cyfrifoldeb Anthem yw sicrhau bod unrhyw hysbysiad o newid mewn perthynas â newid amgylchiadau yn cael ei gofnodi ac y gweithredir arno.

4.4.5 Mae'r Swyddog Diogelu Data (SDD) yn gyfrifol am sicrhau bod gweithdrefnau a pholisïau priodol yn eu lle i gadw data personol yn gywir ac wedi'i ddiweddaru, gan roi ystyriaeth i faint y data a gesglir, pa mor gyflym y gallai newid ac unrhyw ffactorau perthnasol eraill.

4.4.6 O leiaf yn flynyddol, bydd y Swyddog Diogelu Data (SDD) yn adolygu dyddiadau dargadw yr holl ddata personol a brosesir gan Anthem, gan gyfeirio at y rhestr ddata, a bydd yn nodi unrhyw ddata nad oes ei angen mwyach yng nghyd-destun y diben cofrestredig. Bydd y data yma yn cael ei ddileu/dinistrio yn ddiogel yn unol â'r canllawiau ar Waredu Data a Chyfryngau Storio yn Ddiogel, fel sydd wedi'i gyflwyno yn y Weithdrefn Dargadw Data.

4.4.7 Mae'r Swyddog Diogelu Data (SDD) yn gyfrifol am ymateb i geisiadau cywiro gan destunau data o fewn un mis (Gweithdrefn Cais Mynediad Testun, fel sydd wedi'i fanylu yn yr Hysbysiad a Gweithdrefn Preifatrwydd). Gall hyn gael ei ymestyn i ddau fis pellach yn achos ceisiadau cymhleth. Os yw Anthem yn dewis peidio â chydymffurfio â'r cais, rhaid i'r Swyddog Diogel Data (SDD) ymateb i destun y data i esbonio eu rhesymeg a'u hysbysu o'u hawl i gwyno i'r awdurdod goruchwylio a gwneud cais am unioni barnwrol.

4.4.8 Mae'r Swyddog Diogelu Data (SDD) yn gyfrifol am wneud trefniadau priodol, lle y gallai data personol anghywir neu hen fod wedi'i drosglwyddo i sefydliadau trydydd parti, i'w hysbysu bod yr wybodaeth yn anghywir a/neu'n hen ac na ddylid ei ddefnyddio i lywio penderfyniadau ynglŷn â'r unigolion dan sylw; ac am drosglwyddo unrhyw gywiriad i'r data personol i'r trydydd parti lle y bo gofyn gwneud hyn.

4.5 <u>Rhaid i ddata personol gael ei gadw mewn ffurf fel y gall testun y data gael ei adnabod yn unig cyhyd â bod angen er mwyn prosesu.</u>

4.5.1 Lle y caiff data personol ei gadw y tu hwnt i'r dyddiad prosesu, cedwir cyn lleied â phosibl er mwyn diogelu adnabyddiaeth testun y data mewn achos o dor diogelwch data.

4.5.2 Caiff data personol ei gadw yn unol â'r Weithdrefn Dargadw Data ac, unwaith y bydd ei ddyddiad dargadw wedi mynd heibio, rhaid ei ddinistrio'n ddiogel fel sydd wedi'i nodi yn y weithdrefn hon.

4.5.3 Rhaid i'r Swyddog Diogelu Data (SDD) gymeradwyo'n benodol unrhyw achos o ddargadw data sy'n mynd y tu hwnt i'r cyfnodau dargadw a ddiffinnir yn y Weithdrefn Dargadw Data, a rhaid sicrhau bod y cyfiawnhad wedi'i nodi'n glir ac yn

unol â gofynion y ddeddfwriaeth diogelu data. Rhaid i'r gymeradwyaeth hon fod yn ysgrifenedig.

4.6 Rhaid i ddata personol gael ei brosesu mewn modd sy'n sicrhau'r diogelwch priodol

Bydd y Swyddog Diogelu Data (SDD) yn cynnal asesiad risg gan roi ystyriaeth i holl amgylchiadau gweithrediadau rheoli neu brosesu Anthem.

Wrth benderfynu ar briodoldeb, dylai'r Swyddog Diogelu Data (SDD) hefyd ystyried y graddau o niwed neu golled posibl a allai gael ei achosi i unigolion (e.e. staff neu gyfranogwyr) pe byddai tor diogelwch yn digwydd, effaith unrhyw dor diogelwch ar Anthem ei hun, ac unrhyw niwed tebygol i enw da gan gynnwys y posibilrwydd o golli ymddiriedaeth cwsmeriaid.

Wrth asesu mesurau technegol priodol, bydd y Swyddog Diogelu Data (SDD) yn ystyried y canlynol:
- Diogelu â chyfrineiriau;
- Cloi terfynellau segur yn awtomatig;
- Gwaredu hawliau mynediad ar gyfer USB a chyfryngau cof eraill;
- Meddalwedd gwirio am firysau a waliau tân;
- Hawliau mynediad ar sail rôl, gan gynnwys rhai a bennir i staff dros dro;
- Amgryptio dyfeisiau sy'n gadael eiddo'r sefydliad, megis gliniaduron;
- Diogelu rhwydweithiau lleol ac ardal eang;
- Technolegau sy'n gwella preifatrwydd megis rhoi dan ffugenw ac anonymeiddio;
- Nodi safonau diogelwch rhyngwladol priodol sy'n berthnasol i Anthem.

Wrth asesu mesurau sefydliadol priodol, bydd y Swyddog Diogelu Data (SDD) yn ystyried y canlynol:
- Y lefelau hyfforddiant priodol ar draws Anthem;
- Mesurau sy'n ystyried dibynadwyedd cyflogeion (geirdaon ac ati);
- Cynnwys diogelu data mewn contractau cyflogaeth;
- Nodi mesurau camau disgyblu ar gyfer tor diogelwch data;
- Monitro staff mewn perthynas â chydymffurfiaeth â safonau diogelwch perthnasol;
- Rheolaethau mynediad ffisegol i gofnodion electronig a phapur;
- Mabwysiadu polisi desg glir;
- Storio data sydd ar bapur mewn cabinetau gwrthdan y gellir eu cloi;
- Cyfyngu ar ddefnyddio dyfeisiau electronig cludadwy y tu allan i'r gweithlu;
- Cyfyngu ar ddefnyddio dyfeisiau personol y cyflogeion yn y gweithle;
- Mabwysiadu rheolau clir ynglŷn â chyfrineiriau;
- Gwneud copïau wrth gefn yn rheolaidd o ddata personol a storio'r cyfryngau oddi ar y safle;
- Gosod rhwymedigaethau contractiol ar y sefydliadau sy'n mewnforio i gymryd mesurau diogelu priodol wrth drosglwyddo data y tu allan i'r Ardal Economaidd Ewropeaidd.

Mae'r rheoliadau hyn wedi'u dewis ar sail risgiau a nodwyd i ddata personol, a'r posibilrwydd o niwed neu drallod i unigolion y mae eu data yn cael ei brosesu.

4.7 Rhaid i'r rheolydd allu dangos cydymffurfiaeth ag egwyddorion eraill GDPR y DU (atebolrwydd)

Mae GDPR y DU yn cynnwys darpariaethau sy'n hyrwyddo atebolrwydd a llywodraethu. Mae'r rhain yn ategu gofynion tryloywder GDPR y DU. Mae'r egwyddor atebolrwydd yn Erthygl 5(2) yn ei

gwneud yn ofynnol i chi ddangos eich bod yn cydymffurfio â'r egwyddorion ac yn nodi'n benodol mai eich cyfrifoldeb chi yw hyn.

Bydd Anthem yn dangos cydymffurfiaeth â'r egwyddorion diogelu data drwy weithredu polisïau diogelu data, glynu wrth godau ymddygiad, gweithredu mesurau technegol a sefydliadol, yn ogystal â mabwysiadu technegau megis diogelu data drwy ddylunio, Asesiadau o'r Effaith ar Ddiogelu Data, gweithdrefnau hysbysiadau tor diogelwch a chynlluniau ymateb i achosion.

5. Hawliau testunau data

5.1 Mae gan destunau data yr hawliau canlynol mewn perthynas â phrosesu data, a'r data a gofnodir amdanynt:

- 5.1.1 Gwneud cais am fynediad at ddata ynglŷn â natur yr wybodaeth a ddelir ac i bwy y mae wedi'i ddatgelu.
- 5.1.2 Atal prosesu sy'n debygol o achosi niwed neu drallod.
- 5.1.3 Atal prosesu at ddibenion marchnata uniongyrchol.
- 5.1.4 Cael eu hysbysu o fecanwaith proses benderfynu awtomatig a fydd yn effeithio'n sylweddol arnynt.
- 5.1.5 Peidio â chael penderfyniadau sylweddol a fydd yn effeithio arnynt wedi'u gwneud gan broses awtomatig yn unig.
- 5.1.6 Erlyn am iawndal os ydynt yn dioddef niwed drwy unrhyw achos o fynd yn groes i GDPR y DU.
- 5.1.7 Gweithredu i gywiro, blocio, dileu, gan gynnwys yr hawl i gael eu hanghofio, neu ddinistrio data anghywir.
- 5.1.8 Gofyn i'r awdurdod goruchwylio asesu a fu achos o fynd yn groes i unrhyw ddarpariaeth GDPR y DU.
- 5.1.9 Cael data personol wedi'i ddarparu iddynt mewn fformat strwythuredig, cyffredin ei ddefnydd ac a all gael ei ddarllen gan beiriant, a'r hawl i gael y data hwnnw wedi'i drosglwyddo i reolydd arall.
- 5.1.10 Gwrthwynebu i unrhyw broffilio awtomatig sy'n digwydd heb gydsyniad.

5.2 Mae Anthem yn sicrhau y gall testunau data arfer yr hawliau canlynol:

- 5.2.1 Gall testunau data wneud ceisiadau am fynediad at ddata fel a ddisgrifir yn y Weithdrefn ar Gais am Fynediad at Ddata gan y Testun; mae'r weithdrefn hon hefyd yn disgrifio sut bydd Anthem yn sicrhau bod ei hymateb i'r cais am fynediad at ddata yn cydymffurfio â gofynion GDPR y DU.
- 5.2.2 Mae gan destunau data yr hawl i gwyno i Anthem mewn perthynas â phrosesu eu data personol, y modd yr ymdriniwyd â chais gan destun data ac apeliadau gan destun data ar sut yr ymdriniwyd â chwynion yn unol â'r Weithdrefn Gwyno.

6. Cydsyniad

6.1 Mae Anthem yn ystyried bod 'cydsyniad' yn golygu ei fod wedi'i roi yn eglur a rhydd, a bod mynegiant penodol, diamwys ar sail gwybodaeth o ddymuniadau testun y data, drwy ddatganiad neu weithred gadarnhaol glir, yn dangos cytundeb i ddata personol amdanynt gael ei brosesu. Gall testun y data dynnu eu cydsyniad yn ôl ar unrhyw adeg.

6.2 Mae Anthem yn ystyried bod 'cydsyniad' yn golygu bod testun y data wedi'u hysbysu'n llawn o'r prosesu a fwriedir a'u bod wedi nodi eu cytundeb, tra eu bod mewn cyflwr meddwl priodol i wneud hynny a heb i bwysau gael ei roi arnynt. Ni fydd cydsyniad a gafwyd o dan orfodaeth nac ar sail gwybodaeth gamarweiniol yn sail ddilys i brosesu.

6.3 Rhaid bod rhyw gyfathrebu gweithredol rhwng y partïon i ddangos cydsyniad gweithredol. Ni ellir casglu bod cydsyniad wedi'i roi drwy ddiffyg ymateb i gyfathrebiad. Rhaid i'r Rheolydd allu dangos bod cydsyniad wedi'i gael i weithredu'r prosesu.

6.4 Yn achos data sensitif, rhaid cael cydsyniad ysgrifenedig eglur testunau'r data oni bai bod sail ddilys arall i brosesu yn bodoli.

6.5 Yn y rhan fwyaf o achosion, bydd Anthem yn derbyn cydsyniad i brosesu data personol a sensitif yn arferol gan ddefnyddio dogfennau cydsyniad arferol, naill ai'n electronig drwy blatfformau megis Mailchimp, Google Forms neu Survey Monkey, neu ar ffurf copi caled wrth gymryd rhan mewn prosiect.

6.6 Lle y bo Anthem yn darparu gwasanaethau ar-lein i blant, rhaid cael awdurdodiad gan riant neu geidwad. Mae'r gofyniad hwn yn berthnasol i blant o dan 16 mlwydd oed.

6.7 Lle y bo Anthem yn darparu gwasanaethau i oedolion bregus, byddwn yn ystyried y pethau canlynol: wrth ddibynnu ar gydsyniad, gwnawn yn siŵr fod yr oedolyn yn deall i beth maent yn cydsynio, ac ni wnawn gamfanteisio ar unrhyw anghydbwysedd pŵer yn y berthynas rhyngom; wrth ddibynnu ar 'angenrheidiol i gyflawni contract', ystyriwn allu'r oedolyn i ddeall yr hyn maent yn cytuno iddo, ac i fynd i gontract; wrth ddibynnu ar 'buddiannau dilys', cymrwn gyfrifoldeb i nodi risgiau a chanlyniadau'r prosesu, a rhown fesurau diogelu priodol yn eu lle.

7. Diogelwch data

7.1 Mae'r holl Staff yn gyfrifol am sicrhau bod unrhyw ddata personol y mae Anthem yn ei ddal ac y maent yn gyfrifol amdano, yn cael ei gadw'n ddiogel ac na chaiff ei ddatgelu i unrhyw drydydd parti o dan unrhyw amodau oni bai bod y trydydd parti hwnnw wedi'i awdurdodi'n benodol gan Anthem i dderbyn yr wybodaeth honno a bod cytundeb cyfrinachedd yn ei le fel sydd wedi'i gynnwys yn y contract, y Weithdrefn Hysbysiad Preifatrwydd a'r Polisi Dargadw Data.

7.2 Dylai unrhyw ddata personol fod yn hygyrch i'r sawl sydd angen ei ddefnyddio'n unig, ac yn unol â pholisïau diogelu data Anthem yn unig y gellir rhoi mynediad iddo. Dylai unrhyw ddata personol gael ei drin â'r diogelwch pennaf a rhaid ei gadw:

- mewn ystafell y gellir ei chloi a chyda mynediad wedi'i reoli; a/neu
- mewn drôr neu gabinet ffeilio dan glo; a/neu
- os yw'n gyfrifiadurol, wedi'i ddiogelu gan gyfrinair yn unol â gofynion corfforaethol yn y Polisi Rheoli Mynediad; a/neu
- wedi'i storio ar Google Drive ac o bosibl ar gyfryngau cyfrifiadur (symudadwy), ill dau wedi'u hamgryptio yn unol â Gwaredu Cyfryngau Storio yn Ddiogel, fel a nodir yn y Weithdrefn Dargadw Data.

7.3 Rhaid cymryd gofal i sicrhau nad yw sgriniau cyfrifiaduron personol a therfynellau yn weladwy ac eithrio i Staff awdurdodedig Anthem. Mae gofyn i'r holl Staff ddod i Gytundeb Defnydd Derbyniol cyn iddynt gael mynediad i wybodaeth sefydliadol o unrhyw fath, sy'n nodi rheolau ar derfynau amser sgriniau.

7.4 Ni cheir gadael cofnodion llaw mewn unrhyw le lle y gall personél heb eu hawdurdodi gael mynediad iddynt ac ni cheir eu symud o eiddo'r busnes heb awdurdodiad eglur. Unwaith na fydd angen cofnodion llaw i roi cymorth cleientiaid o ddydd i ddydd, rhaid iddynt gael eu

gwaredu o archifau diogel yn unol â chanllawiau Anthem ar waredu data fel a fanylir yn y Weithdrefn Dargadw Data.

7.5 Caiff data personol ei ddileu neu'i waredu yn unol â'r Weithdrefn Dargadw Data yn unig. Bydd cofnodion llaw a ddaeth i'w dyddiad dargadw yn cael eu darnio a'u gwaredu fel 'gwastraff cyfrinachol'. Caiff gyriannau caled cyfrifiaduron personol diangen eu dinistrio ar unwaith fel sy'n ofynnol cyn eu gwaredu.

7.6 Mae prosesu data personol 'oddi ar y safle' yn arwain at risg bosibl fwy o golli, dwyn neu ddifrodi data personol. Rhaid i staff gael eu hawdurdodi'n benodol i brosesu data oddi ar y safle.

8. Datgelu data

8.1 Rhaid i Anthem sicrhau na chaiff data personol ei ddatgelu i drydydd partïon sy'n cynnwys aelodau'r teulu, ffrindiau, cyrff llywodraeth, ac mewn amgylchiadau penodol, yr Heddlu. Dylai'r holl Staff fod yn ofalus pe gofynnir iddynt ddatgelu data personol a ddelir am unigolyn arall i drydydd parti a bydd cydymffurfio â GDPR yn rhwymedigaeth gontractiol. Mae'n bwysig cadw mewn meddwl a yw datgelu'r wybodaeth yn berthnasol i ymgymryd â busnes Anthem ac yn angenrheidiol ar gyfer hynny.

8.2 Rhaid i bob cais i ddarparu data am un o'r rhesyma hyn gael ei ategu gan waith papur priodol a rhaid i bob datgeliad o'r fath gael ei awdurdodi'n benodol gan y Swyddog Diogelu Data (SDD).

9. Dargadw a gwaredu data

9.1 Ni fydd Anthem yn cadw data personol mewn ffurf sy'n caniatáu i adnabod testunau data am gyfnod hirach nag sy'n angenrheidiol, mewn perthynas â'r diben/dibenion y casglwyd y data ato/atynt yn wreiddiol.

9.2 Gallai Anthem storio data am gyfnodau hirach os caiff y data personol ei brosesu'n unig at ddibenion archifo er budd y cyhoedd, at ddibenion ymchwil wyddonol neu hanesyddol, neu at ddibenion ystadegol, yn ddibynnol ar weithredu mesurau technegol a sefydliadol priodol i ddiogelu hawliau a rhyddid testun y data.

9.3 Caiff y cyfnod dargadw ar gyfer pob categori o ddata personol ei nodi yn y Weithdrefn Dargadw Data ynghyd â'r meini prawf a ddefnyddir i bennu'r cyfnod hwn gan gynnwys unrhyw rwymedigaethau statudol sydd gan Anthem i ddargadw'r data.

9.4 Bydd gweithdrefnau dargadw data a gwaredu data Anthem yn berthnasol ym mhob achos.

9.5 Rhaid i ddata personol gael ei waredu yn ddiogel yn unol â chweched egwyddor GDPR – wedi'i brosesu mewn modd priodol i gynnal diogelwch, a thrwy hynny ddiogelu "hawliau a rhyddid" testunau data. Caiff unrhyw achos o waredu data ei wneud yn unol â'r canllawiau gwaredu diogel sydd wedi'u nodi yn y Weithdrefn Dargadw Data.

10. Trosglwyddo data

10.1 Mae allforio data o'r tu mewn i'r DU yn anghyfreithlon oni bai bod lefel briodol o "ddiogelwch ar gyfer hawliau sylfaenol testunau'r data".

Mae trosglwyddiadau cyfyngedig o'r tu mewn i'r DU i wledydd eraill, gan gynnwys i'r Ardal Economaidd Ewropeaidd, bellach yn destun rheolau trosglwyddo o dan gyfundrefn y DU. Mae

rheolau trosglwyddo'r DU yn adlewyrchu'n fras reolau GDPR yr UE, ond mae gan y DU yr annibyniaeth i barhau i adolygu'r fframwaith.

Mae trosglwyddo data personol y tu allan i'r DU wedi'i wahardd oni bai bod un neu ragor o'r mesurau diogelu neu'r eithriadau a nodir, yn berthnasol:

10.1.1 Rheoliadau Digonolrwydd

Mae gan lywodraeth y DU y pŵer i wneud ei 'phenderfyniadau digonolrwydd' ei hun mewn perthynas â thrydydd gwledydd a sefydliadau rhyngwladol. Yng nghyfundrefn y DU, caiff y rhain bellach eu galw'n 'rheoliadau digonolrwydd'.

10.1.2 Tarian Preifatrwydd

Os yw Anthem yn dymuno trosglwyddo data personol o'r DU i sefydliad yn yr Unol Daleithiau dylai wirio bod y sefydliad wedi cofrestru â fframwaith Tarian Preifatrwydd yn Adran Fasnach yr Unol Daleithiau. Mae'r rhwymedigaeth sy'n berthnasol i gwmnïau o dan y Darian Preifatrwydd wedi'u cynnwys yn yr "Egwyddorion Preifatrwydd". Adran Fasnach yr Unol Daleithiau sy'n gyfrifol am reoli a gweinyddu'r Darian Preifatrwydd a sicrhau bod cwmnïau'n cadw at eu hymrwymiadau. Er mwyn ardystio, mae'n rhaid bod gan gwmnïau bolisi preifatrwydd yn unol â'r Egwyddorion Preifatrwydd e.e. defnyddio a storio'r data personol, a'i drosglwyddo ymhellach, yn unol â set gref o reolau a mesurau diogelu data. Mae'r diogelwch a roddir i'r data personol yn berthnasol p'un a yw'r data personol yn ymwneud â phreswylydd y DU neu beidio. Rhaid i sefydliadau adnewyddu eu "haelodaeth" o'r Darian Preifatrwydd yn flynyddol. Os nad ydynt, ni allant mwyach dderbyn a defnyddio data personol o'r DU o dan y fframwaith.

<u>Y rheolydd data i asesu digonolrwydd</u>

Wrth asesu digonolrwydd, dylai'r rheolydd allforio sy'n seiliedig yn y DU ystyried y ffactorau canlynol:

- natur yr wybodaeth sy'n cael ei throsglwyddo;
- gwlad neu diriogaeth tarddiad yr wybodaeth, a'r gyrchfan derfynol;
- sut caiff yr wybodaeth ei defnyddio ac am ba hyd;
- deddfau ac arferion gwlad y trosglwyddai, gan gynnwys codau ymarfer a rhwymedigaethau rhyngwladol perthnasol;
- y mesurau diogelu sydd i'w cymryd mewn perthynas â'r data yn y lleoliad tramor.

<u>10.1.3 Eithriadau</u>

Yn absenoldeb penderfyniad digonolrwydd, aelodaeth o'r Darian Preifatrwydd, rheolau corfforaethol gorfodol a/neu gymalau contract model, ni cheir trosglwyddo data personol i drydydd gwlad na sefydliad rhyngwladol oni bai bod hynny ar un o'r amodau canlynol:

- bod testun y data wedi cydsynio'n eglur i'r trosglwyddiad arfaethedig, ar ôl cael eu hysbysu o risgiau posibl trosglwyddiadau o'r fath i destun y data yn absenoldeb penderfyniad digonolrwydd a mesurau diogelu priodol;
- bod y trosglwyddiad yn angenrheidiol i gyflawni contract rhwng testun y data a'r rheolydd neu weithredu mesurau cyn-gontractiol a gymerwyd ar gais testun y data;

- bod y trosglwyddiad yn angenrheidiol i gwblhau neu gyflawni contract a gwblheir er budd testun y data rhwng y rheolydd a bod dynol neu gyfreithiol arall;
- bod y trosglwyddiad yn angenrheidiol am resymau pwysig yn ymwneud â budd y cyhoedd;
- bod y trosglwyddiad yn angenrheidiol i sefydlu, arfer neu amddiffyn hawliadau cyfreithiol; a/neu
- bod y trosglwyddiad yn angenrheidiol er mwyn diogelu buddiannau hanfodol testun y data neu bersonau eraill, lle y mae testun y data yn gorfforol neu'n gyfreithiol analluog i roi cydsyniad.

11. Cofrestr asedau gwybodaeth

11.1 Mae Anthem wedi sefydlu cofrestr asedau gwybodaeth a phroses llif ddata fel rhan o'i chamau i fynd i'r afael â risgiau a chyfleoedd ar draws ei phrosiect i gydymffurfio â GDPR y DU. Mae rhestr ddata a llif ddata Anthem yn pennu:

- prosesau busnes sy'n defnyddio data personol;
- ffynhonnell data personol;
- disgrifiad o bob eitem o ddata personol;
- gweithgarwch prosesu;
- cynnal categorïau'r rhestr ddata o ddata personol a brosesir;
- dogfennu at ba ddiben/dibenion y caiff pob categori o ddata personol ei ddefnyddio;
- derbynwyr, a derbynwyr posibl, y data personol;
- rôl Anthem ar draws y llif ddata;
- systemau ac ystorfeydd allweddol;
- unrhyw drosglwyddiadau data;
- yr holl ofynion dargadw a gwaredu.

11.2 Mae Anthem yn ymwybodol o unrhyw risgiau sy'n gysylltiedig â phrosesu mathau penodol o ddata personol.

11.2.1 Mae Anthem yn asesu'r lefel o risg i unigolion sy'n gysylltiedig â phrosesu eu data personol. Caiff asesiadau o'r effaith ar ddiogelu data eu cynnal mewn perthynas ag Anthem yn prosesu data personol, ac mewn perthynas â phrosesu a wneir gan sefydliadau eraill ar ran Anthem.

11.2.2 Bydd Anthem yn rheoli unrhyw risgiau a nodir gan yr asesiad risg er mwyn lleihau'r tebygolrwydd o anghydffurfio â'r polisi hwn.

11.2.3 Os yw math o brosesu, yn benodol wrth ddefnyddio technolegau newydd a chan roi ystyriaeth i natur, cwmpas, cyd-destun a dibenion y prosesu, yn debygol o arwain at risg uchel i hawliau a rhyddid bodau dynol, bydd Anthem, cyn y prosesu, yn cynnal asesiad o'r effaith ar ddiogelu yn sgil y gweithrediadau prosesu a ragwelir ar ddiogelu data personol. Gallai asesiad unigol o'r fath fynd i'r afael â set o weithrediadau prosesu tebyg sy'n cyflwyno risgiau uchel tebyg.

11.2.4 Os yw, yn sgil asesiad o'r effaith ar ddiogelu, yn glir bod Anthem ar fin cychwyn prosesu data personol mewn modd a allai achosi niwed a/neu drallod i destunau'r data, rhaid i'r penderfynu ynghylch p'un a yw Anthem am barhau gael ei uwchgyfeirio i'w adolygu gan y Swyddog Diogelu Data (SDD).

11.2.5 Bydd y Swyddog Diogelu Data (SDD), os oes pryderon sylweddol, boed o ran y niwed neu'r trallod posibl, neu o ran ansawdd y data dan sylw, yn uwchgyfeirio'r mater i'r awdurdod goruchwylio.

11.2.6 Bydd rheolaethau yn cael eu dewis a'u cymhwyso i leihau'r lefel o risg sy'n gysylltiedig â phrosesu data unigol i lefel dderbyniol, gan sicrhau bod pawb yn Anthem yn cydymffurfio â gofynion GDPR.

Perchennog y Ddogfen a Chymeradwyo

Y Swyddog Diogelu Data (SDD) yw perchennog y ddogfen hon ac sy'n gyfrifol am sicrhau bod y ddogfen bolisi hon yn cael ei hadolygu yn unol â'r gofynion adolygu a nodir uchod.

Mae fersiwn gyfredol o'r ddogfen hon ar gael i holl aelodau staff yn ffolder Polisïau ar Google Drive Anthem. Bydd unrhyw geisiadau i weld y polisi hwn gan aelodau'r cyhoedd yn cael eu cyflawni.

Cymeradwywyd y polisi hwn gan Fwrdd y Cyfarwyddwyr ar 27^{ain} Ionawr 2021 ac fe'i cyhoeddir ar sail rheoli fersiynau o dan lofnod y Prif Swyddog Gweithredol.

Llofnod: Dyddiad: 27.01.2021
Prif Weithredwr Anthem