



Polisi Diogelu Data

Datganiad polisi

Mae angen i **QAA** gasglu gwybodaeth bersonol i gyflawni ein swyddogaethau a'n gweithgareddau bob-dydd yn effeithiol, ac i ddarparu ein gwasanaethau. Cesglir data o'r fath oddi wrth weithwyr, aelodau, cwsmeriaid, cyflenwyr a chleientiaid, ac mae'n cynnwys (*ond nid yw'n gyfyngedig*)

i) enw, cyfeiriad, cyfeiriad e-bost, dyddiad geni, cyfeiriad IP, rhifau adnabyddiaeth, gwybodaeth breifat a chyfrinachol, gwybodaeth sensitif a manylion banc/cerdyn credyd.

Yn ogystal, mae'n bosib y bydd gofyn i ni gasglu a defnyddio rhai mathau o wybodaeth bersonol i gydymffurfio â gofynion y gyfraith a/neu reoliadau. Fodd bynnag, rydym wedi ymrwmo i brosesu'r holl wybodaeth bersonol yn unol â'r Rheoliad Diogelu Data Cyffredinol (GDPR), cyfreithiau diogelu data'r DU ac unrhyw gyfreithiau a chodau ymddygiad diogelu data perthnasol eraill (y cyfeirir atynt gyda'i gilydd fel '**cyfreithiau diogelu data**').

Mae QAA wedi ymrwmo i sicrhau a chynnal diogelwch a chyfrinachedd data personol a/neu ddata categori arbennig, ac mae pob cydweithiwr yn gyfrifol am drin data yn unol â'r polisi hwn.

Cylch gorchwyl

Pwrpas y polisi hwn yw sicrhau cydymffurfiaeth â *Deddf Diogelu Data (DPA) 2018* a Rheoliad Diogelu Data Cyffredinol (GDPR) (UE) 2016/679, sy'n llywodraethu sut y prosesir unrhyw wybodaeth am unigolion byw a'r hawliau sydd gan yr unigolion hynny mewn perthynas â'r wybodaeth hon. Mae'r ddeddfwriaeth hon yn cwmpasu'r holl wybodaeth bersonol a gedwir ar ffurf electronig ac ar bapur.

Mae QAA yn rheolydd ac yn brosesydd data personol ac mae'r Asiantaeth wedi'i chofrestru gyda Swyddfa'r Comisiynydd Gwybodaeth (ICO) fel Rheolydd Data. Mae'r polisi'n ymgorffori canllawiau gan yr ICO ac yn amlinellu sut y bydd QAA yn cyflawni eu dyletswyddau a'u rhwymedigaethau i gydymffurfio â deddfwriaeth diogelu data.

Mae'r polisi hwn yn berthnasol i bob rhan o QAA ac i'r holl ddata personol a gedwir ac a brosesir gan y sefydliad. Mae hyn yn cynnwys data a gedwir mewn unrhyw system neu fformat, boed yn electronig neu ar bapur.

Mae cadw at y polisi hwn yn orfodol i holl weithwyr QAA gan gynnwys pob aelod o staff parhaol, a'r rhai sydd ar gytundeb cyfnod penodol a dros-dro, adolygwyr, cynrychiolwyr trydydd parti neu is-contractwyr, gweithwyr asiantaeth, gwirfoddolwyr, interniaid ac asiantau sy'n ymwneud â QAA yn y DU neu dramor. Gallai peidio â chydymffurfio arwain at gamau disgyblu.

Categoriâu o ddata

At ddibenion categoreiddio gwybodaeth, mae QAA yn defnyddio diffiniadau GDPR o 'ddata personol' a 'data categori arbennig', fel a ganlyn:

Data personol	Data categori arbennig
<p>Unrhyw wybodaeth sy'n ymwneud â pherson naturiol a adnabyddir neu sy'n adnabyddadwy.</p> <p>Person naturiol adnabyddadwy yw rhywun y gellir ei adnabod, yn uniongyrchol neu'n anuniongyrchol, yn benodol trwy gyfeirio at ddynodwr fel:</p> <ul style="list-style-type: none">• enw• rhif adnabyddiaeth• data'n ymwneud â lleoliad• dynodwr ar-lein, neu• un neu fwy o ffactorau sy'n perthyn yn benodol i hunaniaeth gorfforol, ffisiolegol, genetig, meddyliol, economaidd, diwylliannol neu gymdeithasol y person naturiol hwnnw.	<p>Data personol sy'n datgelu neu'n ymwneud â pherson naturiol adnabyddadwy:</p> <ul style="list-style-type: none">• tarddiad hiliol neu ethnig• safbwyntiau gwleidyddol• credoau crefyddol neu athronyddol• aelodaeth o undeb llafur• iechyd• bywyd rhywiol neu gyfeiriadedd rhywiol, neu• brosesu data genetig neu ddata biometrig at ddiben adnabod person naturiol yn unigryw.

Mae QAA yn sicrhau bod data personol sy'n dod o fewn '**categoriâu arbennig**' GDPR yn cael ei drin â lefel arbennig o uchel o ran gofal, oherwydd y dybiaeth y gallai'r math hwn o wybodaeth gael ei defnyddio mewn ffordd negyddol neu gamwahaniaethol a'i bod o natur sensitif a phersonol i'r personau y mae'n ymwneud â nhw. Mae QAA yn gwneud cyn lleied â phosib o brosesu data categori arbennig i'n galluogi i gyflawni ein swyddogaethau.

Egwyddorion diogelu data

Mae Erthygl 5(2) o GDPR yn ei gwneud yn ofynnol i QAA, eu gweithwyr ac eraill sy'n prosesu neu'n defnyddio unrhyw wybodaeth personol fod yn gyfrifol am, ac yn gallu dangos, cydymffurfiaeth â'r egwyddorion diogelu data.

Mae'r egwyddorion diogelu data yn nodi y dylai data personol:

- cael ei brosesu'n gyfreithlon, yn deg ac mewn modd tryloyw mewn perthynas ag unigolion
- cael ei gasglu at ddibenion penodol, eglur a chyfreithlon a heb ei brosesu ymhellach mewn modd sy'n anghydnaws â'r dibenion hynny
- bod yn ddigonol, yn berthnasol ac yn gyfyngedig i'r hyn sy'n angenrheidiol mewn perthynas â'r dibenion y caiff ei brosesu ar eu cyfer
- bod yn gywir a lle bo angen yn cael ei gadw'n gyfredol. Rhaid cymryd pob cam rhesymol i sicrhau bod data personol sy'n anghywir, gan ystyried y dibenion y'i prosesir ar eu cyfer, yn cael ei ddileu neu ei gywiro'n ddi-oed.
- cael ei gadw ar ffurf nad yw'n caniatáu adnabod testunau data am gyfnod hwy nag sy'n angenrheidiol at y dibenion y mae'r data'n cael ei brosesu ar eu cyfer
- cael ei brosesu mewn modd sy'n sicrhau diogelwch priodol y data personol gan gynnwys amddiffyniad yn erbyn prosesu anawdurdodedig neu anghyfreithlon ac yn erbyn colled, dinistr neu ddifrod damweiniol, gan ddefnyddio mesurau technegol neu sefydliadol priodol.

Polisi QAA yw y dylai prosesu pob data personol fod yn ddiogel, yn foesechol ac yn dryloyw, ac mae gennym weithdrefnau yn eu lle i alluogi'r sawl sy'n destun y data hwnnw i arfer eu hawliau.

- Rydym yn diogelu hawliau unigolion o ran prosesu gwybodaeth bersonol.
- Rydym yn datblygu, gweithredu a chynnal Polisi Diogelu Data, yn ogystal â gweithdrefn a hyfforddiant ar gyfer cydymffurfio â chyfreithiau diogelu data.
- Rydym yn cofnodi caniatâd ar yr adeg y ceir gafael ar y data, a gallwn roi tystiolaeth o ganiatâd o'r fath pan ofynnir amdano.
- Mae gennym bolisiâu cadarn ac wedi'u dogfennu ar gyfer Adrodd am Gwynion a Digwyddiadau'n ymwneud â Data o ran nodi, ymchwilio, adolygu ac adrodd am unrhyw wallau o ran diogelu data neu gwynion amdanynt.
- Rydym yn storio ac yn dinistrio'r holl wybodaeth bersonol yn unol â'n Polisi Cadw.
- Bydd unrhyw wybodaeth a ddarperir i unigolyn mewn perthynas â data personol a gedwir neu a ddefnyddir amdano, yn cael ei darparu mewn ffurf gryno, dryloyw, ddealladwy a hygyrch, gan ddefnyddio iaith glir a phlaen.
- Rydym yn cadw cofnodion o weithgareddau prosesu.

Cofnodion prosesu lle mae QAA yn Rheolydd Data neu'n Brosesydd Data

Lle rydym yn gweithredu fel Rheolydd Data neu Brosesydd Data (*neu gynrychiolydd*), bydd ein cofnodion mewnol o'r categorïau o weithgareddau prosesu a gynhelir yn cynnwys y wybodaeth ganlynol:

- Enw llawn a manylion cyswllt y prosesydd a phob rheolydd y mae'r prosesydd yn gweithredu ar ei ran, a, lle bo'n berthnasol, cynrychiolydd y rheolydd neu gynrychiolydd y prosesydd, a'r swyddog diogelu data.
- Y categorïau prosesu a gynhelir ar ran pob rheolydd.
- Lle bo'n berthnasol, unrhyw achos lle trosglwyddir data personol i drydedd wlad neu sefydliad rhyngwladol (gan gynnwys nodi'r drydedd wlad neu'r sefydliad rhyngwladol hwnnw a, lle bo'n berthnasol, dogfennu mesurau diogelu addas).
- Disgrifiad cyffredinol o'r mesurau diogelwch ar gyfer prosesu a ddefnyddiwyd (yn unol ag Erthygl 32(1) o'r deddfau diogelu data).

Ardystio allanol

Mae QAA wedi'u hardystio gan Biwrô Asesu Prydain i ISO 27001:2013 sy'n dangos ein bod wedi ymrwmo i, ac yn gwneud pob ymdrech i reoli, ein darpariaethau diogelu data yn unol ag arfer gorau rhyngwladol.

Proseswyr trydydd parti

Mae QAA yn defnyddio proseswyr allanol ar gyfer rhai gweithgareddau prosesu. Rydym yn defnyddio archwiliadau gwybodaeth i ddynodi, categoreiddio a chofnodi'r holl ddata personol sy'n cael ei brosesu y tu allan i QAA, fel bod y wybodaeth, y gweithgaredd prosesu, y prosesydd a'r sail gyfreithiol i gyd yn cael eu cofnodi, eu hadolygu a'u bod ar gael yn hawdd. Gall prosesu allanol o'r fath gynnwys (ond heb fod yn gyfyngedig i) y canlynol:

- Systemau a Gwasanaethau TG
- Gwasanaethau Cyfreithiol
- Cyflogres
- Gwiriadau Cynladwyedd Ariannol, Rheolaeth a Llywodraethiant
- Gwasanaethau Marchnata/Postio Uniongyrchol.

Mae gennym weithdrefnau a mesurau diwydrwydd dyladwy ar waith ac rydym yn adolygu, asesu a gwirio cefndir pob prosesydd cyn ffurfio perthynas fusnes. Yn ystod y gwiriadau hyn, mae'n bosib y byddwn yn cael gafael ar ddogfennau cwmni, ardystiadau a thystlythyrau i sicrhau bod y prosesydd yn ddigonol, yn briodol ac yn effeithiol ar gyfer y dasg rydym yn eu cyflogi ar ei chyfer.

Rydym yn sicrhau bod Cytundebau Lefel Gwasanaeth (SLA) a chontractau sy'n cynnwys rhwymedigaethau cydymffurfio priodol ar waith gyda'r holl broseswyr data trwy'r broses ar gyfer cymeradwyo contractau. Caiff proseswyr eu hysbysu na ddylent gyflogi prosesydd arall heb ein caniatâd penodol ymlaen llaw, a rhaid cyflwyno unrhyw newidiadau y bwriedir eu gwneud ynghylch ychwanegu neu amnewid proseswyr presennol yn ysgrifenedig, cyn i unrhyw newidiadau o'r fath gael eu gweithredu.

Cyfrifoldeb rheolwr y contract yw sicrhau bod pob un o'r gweithgareddau prosesu a nodir yn y contract yn cael eu monitro, eu harchwilio a'u bod yn adrodd arnynt.

Hawliau testun data

Yr hawliau a roddir i'r rhai sy'n destun data o dan ddeddfwriaeth diogelu data yw:

- yr hawl i gael gwybodaeth
- yr hawl i gael mynediad at y wybodaeth a gedwir amdanynt (trwy Gais am Wybodaeth gan Destun)
- yr hawl i gywiro gwallau
- yr hawl i ddileu
- yr hawl i gyfyngu ar brosesu
- yr hawl i gludo data gyda nhw
- yr hawl i wrthwynebu
- hawliau mewn perthynas â gwneud penderfyniadau a phroffilio awtomataidd.

O dan ddeddfwriaeth diogelu data, mae gan unrhyw un sy'n destun data hawl i weld eu data personol a gedwir gan QAA.

Dylai unrhyw unigolyn sy'n dymuno arfer yr hawl hon wneud y cais trwy gyflwyno [Ffurflen Gais am Wybodaeth gan Destun](#) sydd ar gael ar wefan QAA, neu trwy gysylltu â Governance@qaa.ac.uk.

Llywodraethiant data

Data personol am weithwyr

Nid ydym yn defnyddio caniatâd fel sail gyfreithiol ar gyfer cael gafael ar neu brosesu gwybodaeth bersonol am weithwyr. Mae ein polisiau AD wedi cael eu diweddarau i sicrhau bod gweithwyr yn cael y wybodaeth briodol am sut rydym yn prosesu eu data a pham.

Hysbysiad Preifatrwydd

Mae [Hysbysiad Preifatrwydd QAA](#) yn cynnwys yr hyn y gellir ei ddisgwyl pan fo QAA yn casglu gwybodaeth bersonol i fodloni ein rhwymedigaethau cyfreithiol, rheoliadol, statudol a chytundebol ac i ddarparu gwybodaeth i chi, naill ai am ein gwasanaethau neu am faterion sydd o fudd i'r cyhoedd. Mae'r Hysbysiad Preifatrwydd hefyd yn hysbysu gweithwyr am eu hawliau o dan y deddfau diogelu data a sut i arfer yr hawliau hyn; mae hefyd yn manylu ar y wybodaeth bersonol rydym yn ei chasglu a'i phrosesu amdanynt. Mae gennym hefyd Hysbysiad Preifatrwydd ar gyfer Prosesu'r Gyflogres a gyhoeddir yn adran Polisiau ein Mewnwyd.

Storio data

Bydd gwybodaeth a chofnodion sy'n ymwneud â thestun y data yn cael eu storio'n ddiogel, a dim ond gweithwyr awdurdodedig fydd yn cael mynediad atynt. Bydd gwybodaeth yn cael ei storio dim ond cyhyd ag y mae ei hangen neu'r hyn sy'n ofynnol dan y gyfraith, a bydd yn cael ei gwaredu'n briodol.

Cywirdeb data

Mae QAA yn cymryd camau rhesymol i sicrhau bod y wybodaeth hon yn cael ei diweddarau trwy ofyn i destun y data ynghylch unrhyw newidiadau.

Archwiliadau a monitro

Rydym yn cynnal archwiliadau rheolaidd a phrosesau monitro cydymffurfiaeth gyda'r nod o sicrhau bod y mesurau a'r rheolaethau sydd ar waith i ddiogelu'r rhai sy'n destun data a'u gwybodaeth yn ddigonol, yn effeithiol ac yn cydymffurfio â'r gofynion bob amser. Mae QAA yn atebol i'r Pwyllgor Archwilio a Risg, ac yn y pen draw i'r Bwrdd, o ran cydymffurfio â'r polisi hwn.

Hyfforddiant

Mae QAA wedi ymrwymo i sicrhau bod yr holl weithwyr yn deall a bod ganddynt fynediad at eu rhwymedigaethau o dan gyfreithiau ac egwyddorion diogelu data, a'u bod yn cael hyfforddiant a chymorth parhaus i sicrhau a dangos eu gwybodaeth a'u cymhwysedd.

Mae aelodau staff newydd a'r rhai sydd wedi gweithio i QAA ers amser yn cael eu hyfforddi, eu hasesu a'u cynorthwyo i gyflawni eu cyfrifoldebau diogelu data mewn amryw o ffyrdd, gan gynnwys:

- Yn ystod y cyfnod sefydlu.
- Mae pob unigolyn yn cwblhau hyfforddiant ar-lein blynyddol ar gyfer GDPR ac Ymwybyddiaeth o Seiberddiogelwch, gan gynnwys prawf ar ddiwedd pob modiwl.
- Hyfforddiant gloywi blynyddol ar ddiogelu data, rheoli cofnodion a diogelwch gwybodaeth a ddarperir mewn sesiynau grŵp, naill ai wyneb-yn-wyneb neu'n rhithiol.
- Sesiynau cymorth 1 i 1.
- Mynediad at bolisiâu, gweithdrefnau, rhestrau gwirio a dogfennau ategol yn ymwneud â diogelu data a diogelwch gwybodaeth.

Cosbau am beidio â chydymffurfio

Mae QAA yn deall eu rhwymedigaethau a'u cyfrifoldebau o dan y deddfau diogelu data ac yn cydnabod difrifoldeb mynd yn groes i unrhyw un o'r rhain. Rydym yn parchu awdurdod y Comisiynydd Gwybodaeth i osod a gorfodi dirwyon a chosbau arnom pan fyddwn yn methu â chydymffurfio â'r rheoliadau, yn methu â lliniaru'r risgiau lle bo'n bosibl ac yn gweithredu mewn modd sydd, yn fwiadol, ddim yn cydymffurfio.

Dylai gweithwyr nodi difrifoldeb cosbau o'r fath a'r faith eu bod yn gymesur â natur y drosedd, gan gynnwys y canlynol:

Math o drosedd	Uchafswm y ddirwy
Gweithredu'n groes i rwymedigaethau'r rheolydd, y prosesydd, y corff ardystio a'r corff monitro.	Dirwyon gweinyddol hyd at €10,000,000 neu 2% o gyfanswm trosiant blynyddol byd-eang y flwyddyn ariannol flaenorol, pa un bynnag sydd uchaf.
Gweithredu'n groes i'r egwyddorion sylfaenol ar gyfer prosesu, amodau ar gyfer caniatâd, hawliau testun y data, trosglwyddo data personol i dderbynnnydd mewn trydedd wlad neu sefydliad rhyngwladol, sefyllfaoedd prosesu penodol neu beidio â chydymffurfio â gorchymyn gan y Comisiynydd Gwybodaeth.	Dirwyon gweinyddol hyd at €20,000,000 neu 4 % o gyfanswm trosiant blynyddol byd-eang y flwyddyn ariannol flaenorol, pa un bynnag sydd uchaf.

Rolau a chyfrifoldebau

Fel Rheolydd Data (neu wrth weithredu fel Rheolydd Data neu Brosesydd Data ar y cyd), mae gan QAA gyfrifoldeb corfforaethol am y canlynol:

- cydymffurfio â deddfwriaeth diogelu data a chadw cofnodion i ddangos hyn
- cydweithredu â'r ICO, rheoleiddiwr deddfwriaeth diogelu data'r DU
- ymateb i gamau rheoleiddiol/cyfreithiol a thalu ardollau gweinyddol a dirwyon a osodir gan yr ICO.

Caiff rheolau a chyfrifoldebau eu diffinio fel a ganlyn:

Prif Weithredwr

Mae QAA yn Rheolydd Data, a'r Prif Weithredwr sy'n gyfrifol yn y pen draw am sicrhau bod gofynion cyfreithiau diogelu data yn cael eu bodloni a bod y sefydliad yn darparu adnoddau digonol i alluogi'r cwmni a'i holl weithwyr i gydymffurfio â'u dyletswyddau diogelu data.

Grŵp Llywodraethiant Data a Gwybodaeth (DIGG)

Mae DIGG yn monitro cydymffurfiaeth â chyfreithiau diogelu data a pholisïau mewnol sy'n ymwneud ag archwilio diogelu data. Mae DIGG hefyd yn adolygu diogelu data, cadw data ac yn cadw cofnod o bolisïau rheoli, yn ogystal â gwneud argymhellion i'r Prif Weithredwr eu cymeradwyo.

Swyddog Diogelu Data (DPO)

Cyfarwyddwr Cyllid QAA yw'r DPO ac mae'n gyfrifol am y canlynol:

- cydweithredu â'r awdurdod goruchwyllo
- adrodd yn rheolaidd i'r Pwyllgor Gwaith/Bwrdd yng nghyd-destun dynodi a rheoli risgiau gweithredol a strategol.
- cyflwyno adroddiadau blynyddol ar berfformiad i Bwyllgor Archwilio a Risg QAA.

Rheolwr Cyfleusterau a Chydymffurfiaeth

Mae'n gwneud y canlynol:

- cyfeirio materion at gynghorwyr cyfreithiol allanol ac arbenigwyr pwnc *Jisc* fel y bo'n briodol.
- ymchwilio i ddigwyddiadau sy'n ymwneud â data ac yn adrodd ar ganfyddiadau ac argymhellion i'r DPO.
- cynghori ar asesiadau effaith diogelu data ac yn monitro perfformiad yr asesiadau.
- goruchwyllo rheoli cofnodion data a hyfforddi gweithwyr.

Y rhai a gyflogir

Mae'n gyfrifoldeb ar bob gweithiwr i:

- sicrhau eu bod yn casglu, storio a phrosesu data personol yn unol â chyfreithiau diogelu data ac yn cydymffurfio â Pholisi Diogelu Data QAA
- defnyddio data personol dim ond at ddiben y dyletswyddau hynny sy'n perthyn i'w contract cyflogaeth
- cadw data personol yn ddiogel, gan gynnwys dilyn polisiau a phrosesau perthnasol y cwmni
- storio cysylltiadau mewn systemau a gymeradwyir ac a reolir, a pheidio â chadw copïau wedi'u dyblygu yn unman arall
- peidio â cheisio cael mynediad at wybodaeth nad yw'n angenrheidiol iddynt ei chadw, ei gwybod na'i phrosesu
- sicrhau bod unrhyw ddata personol sy'n dod i law yn gywir ac yn berthnasol i'r diben y mae'n angenrheidiol ar ei gyfer
- cwblhau hyfforddiant gorfodol yn llwyddiannus.

Adolygiad polisi

Caiff y polisi hwn ei ddiweddarau o leiaf bob dwy flynedd neu yn ôl yr angen i adlewyrchu arfer gorau, cyfraith achosion berthnasol, ac i sicrhau cydymffurfiaeth ag unrhyw newidiadau neu ddiwygiadau mewn deddfwriaeth diogelu data.

Cyhoeddwyd - 10 Mehefin 2021

© Yr Asiantaeth Sicrhau Ansawdd mewn Addysg Uwch
2021 Rhifau elusen cofrestredig 1062746 a SC037786
www.qaa.ac.uk