IPCO
Investigatory Powers Commissioner's Office
PO Box 29105, London
SW1V 1ZU

Drwy E-bost

Ebrill 2020

Annwyl Syr/Fadam,

Sicrwydd ynghylch Trefniadau Diogelu Trin a Chadw Data

Yng ngoleuni methiannau cydymffurfio difrifol diweddar gan ran o gymuned gudd-wybodaeth y DU, rwyf wedi gofyn i arolygiaeth IPCO gynnal adolygiad llawn o'r ffyrdd yr ymdrinnir â data gan yr awdurdodau cyhoeddus yr ydym yn eu goruchwylio. Mae'r gwaith hwn, a gychwynnodd ddiwedd 2019, wedi golygu cynnal trafodaethau cychwynnol gydag ystod o awdurdodau mewn perthynas â'r data a gedwir ganddynt. Mae hyn yn cynnwys unrhyw ddata a gafwyd dan Ddeddf Pwerau Ymchwilio 2016 a Deddf Rheoleiddio Pwerau Ymchwilio 2000 ac sydd felly yn destun goruchwylio gan fy swyddfa. Bwriedir i'r rhaglen hon hyrwyddo cydymffurfiaeth â'r deddfau hyn a'r Codau Ymarfer, a chyda rhwymedigaethau cyfreithiol eraill gan gynnwys Deddf Diogelu Data 2018. Byddwch yn ymwybodol bod y cyfyngiadau cyfredol wedi golygu bod ein model gweithio wedi newid ac y bydd unrhyw gyswllt â'n harolygwyr yn cael ei gynnal o bell hyd y gellir gweld. Fodd bynnag, bydd fy arolygwyr yn cysylltu â chi i drafod sicrwydd data ochr yn ochr â'n harolygiadau arferol.

Amcanion y rhaglen Sicrwydd Data yw:

- Arolygu ac ymchwilio cydymffurfiaeth â threfniadau diogelu data er mwyn sefydlu lefel uchel o hyder bod yr holl ddata a geir dan y pwerau a gaiff eu goruchwylio gan IPCO yn cael ei gadw'n gyfreithlon.
- Er mwyn sefydlu ac annog arferion gorau ar gyfer cydymffurfio ym mhob awdurdod yr ydym yn ei oruchwylio.
- Er mwyn cynorthwyo'r awdurdodau yr ydym yn eu goruchwylio i ddeall ac archwilio'r heriau cydymffurfio sy'n codi yn sgil y defnydd o raglenni trin data pwrpasol, oddi ar y silff a rhai a rennir, ac amgylcheddau storio technegol.

Mae fy arolygwyr wedi nodi bod nifer o sefydliadau yn cadw data yn hirach nag sydd raid neu'n briodol am nifer o resymau. Yn gyntaf, mewn nifer o achosion, nid yw awdurdodau wedi rhoi polisïau cadw a gwaredu data ar waith yn llawn. Yn ail, mae nifer o awdurdodau'n gweithredu mewn diwylliant o gadw cynhwysfawr i atal colli data gweithredol ac yn olaf, mae'n bosibl na all systemau a ddefnyddir i drosglwyddo a storio data yn ddiogel hyrwyddo neu alluogi prosesau gwaredu priodol.

Er enghraifft, ystyriwch bod awdurdod yn ceisio ac yn cael awdurdodiad ar gyfer gwyliadwriaeth gyfeiriedig. Dan yr awdurdodiad hwnnw, cynhelir goruchwyliaeth am gyfnod o amser gan roi gwybodaeth i fodloni amcanion yr ymchwiliad. Fel rhan o'r ymchwiliad, mae un swyddog yn e-bostio canlyniadau'r oruchwyliaeth i gydweithiwr a'i reolwr ac mae'r ddau yn cadw copi ar eu bwrdd gwaith ac yn Outlook i gyfeirio ato yn y dyfodol. Mae'r swyddog hefyd yn e-bostio'r cynnyrch i gydweithiwr cyfreithiol fel y gellir defnyddio'r cynnyrch yn dystiolaeth yn ystod achos troseddol; caiff ei ddatgelu i lys, felly, a'i gadw mewn ffeil a ddiogelir gan gyfrinair i'w ddefnyddio eto petai apêl. Ar y pwynt hwn, ni chaiff penderfyniad ei wneud ynghylch pa mor hir y dylid cadw'r data, ac mae'r copïau ar Outlook ac ar y bwrdd gwaith yn cael eu cadw.

Er bod yr enghraifft hon yn dangos defnydd dilys o'r data at ddefnydd ymchwiliol a thystiolaethol, mae'n annhebygol bod y dull hwn yn cydymffurfio â'r cod ymarfer ar gyfer gwyliadwriaeth. Mae'r llwybr data a ddisgrifir yn cynnwys cadw ar fwrdd gwaith personol ac Outlook yn ogystal â chadw copi a ddiogelir gan gyfrinair at ddibenion tystiolaethol. Yn yr enghraifft hon, nid oes proses gadw, adolygu neu waredu yn ei lle ar gyfer yr un o'r llwybrau. Mewn achosion fel hyn, mae fy arolygwyr wedi canfod bod data yn cael ei gadw'n hirach nag sydd raid ac, ar adegau, am gyfnod amhenodol. Rwy'n pwyso arnoch i adolygu eich rhwymedigaethau dan IPA a RIPA ac i ailedrych ar y trefniadau diogelu yn y Codau Ymarfer[1] i wneud yn siŵr bod polisïau a phrosesau priodol yn eu lle yn eich awdurdod.

Gan ddechrau yn 2020, bydd arolygiadau IPCO yn cynnwys sicrwydd data a bydd gofyn i'r canlynol fod ar gael i fy arolygwyr: polisïau diogelu; atodlenni cadw a gwaredu; mynediad i unrhyw system a ddefnyddir i storio data a gafwyd dan IPA a RIPA. Trwy gydol pob arolygiad, bydd fy swyddfa yn gofyn i chi ddangos pa mor ddigonol yw eich polisïau gan gynnwys diogelwch ffisegol data, digonolrwydd hyfforddiant staff, camau i leihau copïo data a phrosesau i wneud yn siŵr bod yr holl ddata a chopïau perthnasol yn cael eu dileu ar yr adeg briodol.

Mae'r gwaith hwn yn rhan ganolog o rôl IPCA i gynorthwyo awdurdodau cyhoeddus i ddefnyddio'r pwerau hyn yn gyfreithlon, er budd y cyhoedd. Rwy'n disgwyl y bydd y rhaglen hon yn caniatáu i fy swyddfa sefydlu lefel dda o hyder yn arferion diogelu yr awdurdodau yr wyf yn eu goruchwylio. Rwy'n argymell eich bod yn cymryd y camau a ganlyn, a fydd yn eich cynorthwyo i ddangos cydymffurfiaeth ac ymlyniad at eich rhwymedigaethau i ddiogelu unrhyw ddata yr ydych wedi'i chael neu y gallech ei chael:

1) Adolygu'r rhwymedigaethau diogelu yn y Cod Ymarfer perthnasol ar gyfer unrhyw bŵer a ddefnyddir gan eich awdurdod.
2) Gwneud yn siŵr bod polisïau diogelu mewnol ar gyfer cadw, adolygu a gwaredu unrhyw ddata perthnasol yn gywir a chyfredol.
3) Gwneud yn siŵr bod gan swyddog awdurdodi eich awdurdod ddealltwriaeth lawn o unrhyw lwybr data[2] a ddefnyddir ar gyfer data RIPA neu IPA.
4) Gwneud yn siŵr bod yr holl ddata a geir dan IPA a RIPA wedi'i labelu'n glir a'i storio ar lwybr data ag iddo bolisi cadw hysbys.
5) Adolygu geiriad trefniadau diogelwch mewn unrhyw gymhwysiad i gael data dan IPA a RIPA a gwneud yn siŵr eu bod yn adlewyrchu'n gywir y prosesau cadw a gwaredu yn eich awdurdod[3].
6) Adolygu a yw'r data a geir dan awdurdodiadau blaenorol yn cael ei gadw'n hirach nag sydd raid a, lle'n briodol, ystyried gwaredu data a gedwir.

Os oes gennych unrhyw gwestiwn ynghylch y rhaglen hon neu'r argymhellion sydd gennym, peidiwch petruso cysylltu â IPCO ar Info@IPCO.org.uk. Er nad ydym yn cynnal arolygiadau wyneb yn wyneb, mae fy arolygwyr ar gael i ateb unrhyw gwestiwn sydd gennych, a byddant yn cynnal arolygiadau o bell, ar sail dreigl, drwy gydol y flwyddyn.

Yn gywir

Y Gwir Anrhydeddus Syr Brian Leveson
Comisiynydd Pwerau Ymchwilio

[1] Mae Pennod 13 Cod Ymarfer Data Cyfathrebu, Pennod 8 Cod Ymarfer CHIS a Phennod 9 Cod Ymarfer Goruchwyliaeth ac Ymyrraeth Eiddo yn nodi'r gofynion o ran diogelu.

[2] Er enghraifft, gellir storio data goruchwyliaeth gyfeiriedig ar nifer o lwybrau data yr un pryd: Llwybr un – caiff cynnyrch fideo teledu cylch cyfyng ei drosglwyddo i CD a'i gadw mewn cwpwrdd diogel; Llwybr dau - anfonir copi o'r fideo drwy e-bost a'i storio ar yriant storio cyffredin; Llwybr tri - derbynnir copi o'r fideo drwy e-bost a'i gadw mewn ffolder Outlook gan swyddog cyfreithiol; Llwybr pedwar - derbynnir copi o'r fideo drwy e-bost a'i storio mewn ffolder gwaith achos a ddiogelir â chyfrinair gan swyddog cyfreithiol fel tystiolaeth.

[3] Er enghraifft, os cedwir yr holl ddata am nifer penodedig o flynyddoedd, dylid nodi hyn yn eich cais neu dylai'r cais gyfeirio at y ddogfen Polisi Diogelwch Mewnol.