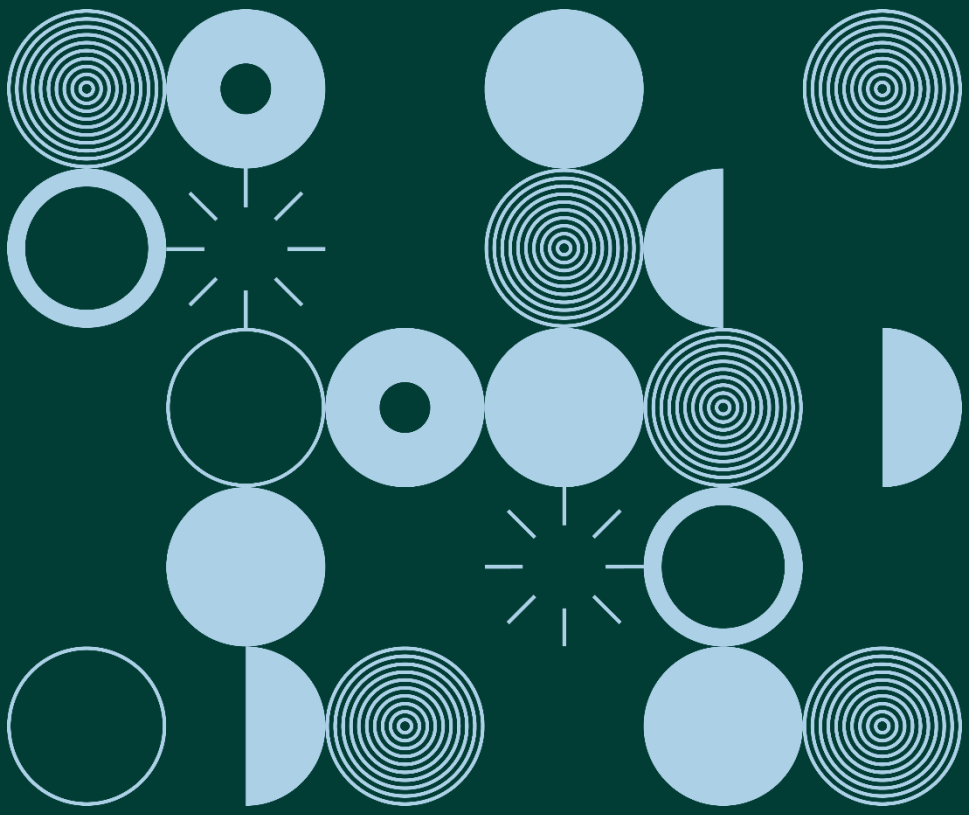
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Nóta Treorach:

Treoir Phraiticiúil ar Fhógraí Sáraithe i ndáil le Sonraí Pearsanta faoin GDPR

Iúil 2019



Treoir Phraiticiúil ar Fhógraí Sáraithe Sonraí Pearsanta faoin GDPR

Clár an Ábhair

Réamhrá

Tá sé i gceist go príomha leis an nóta treorach seo comhairle phraiticiúil a thabhairt do rialaitheoirí sonraí maidir leis an mbealach le sáruithe sonraí a láimhseáil agus le réimeas éigeantach fógartha sárú sonraí a stiúradh, a thug an Rialachán Ginearálta maidir le Cosaint Sonraí (GDPR) isteach i mí na Bealtaine 2018. D'fhéadfadh an treoir seo cuidiú leis an bpobal i gcoitinne freisin sa chás go dtagann údair imní chun cinn maidir le comhlíonadh an réimis i ndáil le sáruithe.

Cuireadh an treoir seo ar fáil tar éis anailís a dhéanamh ar threochtaí agus ar staitisticí a bhreithnigh an Coimisiún um Chosaint Sonraí (DPC) le linn na chéad bhliana de réimeas tuairiscithe éigeandála maidir le sárú a thuairisciú an GDPR. Chlúdaigh na staitisticí agus na treochtaí a rinneadh anailís orthu na fógraí sáraithe sonraí a fuarthas sa chéad bhliain ón 25 Bealtaine 2018, agus tá na mionsonraí leagtha amach i nóta faisnéise ar leith foilsithe ag an DPC.

Thug Aonad Measúnaithe Sáraithe an DPC faoi anailís ar na fógraí sáraithe a fuarthas ó na réimsí éagsúla laistigh den earnáil phoiblí agus phríobháideach, lena n-áirítear, baincéireacht agus airgeadas; árachas; teileachumarsáid; cúram sláinte; agus forfheidhmiú dlí.

Áirítear ar roinnt de na treochtaí agus na saincheisteanna a d'aithin an tAonad Measúnaithe Sáraithe le linn dóibh a bheith ag tabhairt faoi na hathbhreithnithe agus ó láimhsiú fógraí sáraithe: fógraí a bhí deireanach, deacracht ó thaobh measúnú a dhéanamh ar rátálacha riosca, mainneachtain sárú a chur in iúl do na hábhair sonraí, sa chás gur infheidhme; fógraí maidir le sáruithe á ndéanamh arís is arís eile; agus tuairisciú nach raibh leordhóthanach.

Leagtar an treoir thíos amach chun cuidiú le rialaitheoirí a gcuid oibleagáidí maidir le ceanglais fógra agus cumarsáide a thuiscint níos fearr – clúdaítear fógraí chuig an DPC, agus cumarsáid leis na hábhair sonraí freisin, sa chás gur infheidhme – agus le soiléireacht a dhéanamh ar na saincheisteanna is coitianta a tháinig chun cinn le linn na chéad bhliana den réimeas an GDPR ó thaobh fógra i ndáil le sárú a thabhairt.

Molann an DPC freisin go ndéanfaidh na rialaitheoirí sonraí an treoir mionsonraithe atá curtha ar fáil ar ábhair a léamh, lena n-áirítear, an sainmhíniú ar shárú sonraí pearsanta, measúnú fógra maidir le riosca agus riachtanais chumarsáide agus cuntasachta, atá le

fáil sa Mheitheal Oibre Airteagal 29 'treoirlínte ar fhógra i ndáil le sonraí pearsanta a shárú'.[1]

[1] Tháinig an Bord Eorpach um Chosaint Sonra (EDPB), a thacaigh leis na treoirlínte seo, in áit Mheitheal Oibre Airteagal 29.

Léargas Ginearálta ar an Réimeas chun Fógra i ndáil le Sárú a Thabhairt

Roimh bhogadh ar aghaidh chuig an treoir phraiticiúil ar shaincheisteanna coitianta a tháinig aníos i gcomhthéacs fógraí maidir le sárú sonraí, is fiú léargas ginearálta den réimeas fógra maidir le sárú a leagan amach as féin, ar mhaithe lena chinntiú go bhfuil na rialaitheoirí go léir ar an eolas maidir lena gcuid oibleagáidí bunúsacha faoin réimeas seo. Tá ar chumas rialaitheoirí faisnéis a fháil freisin maidir le fógraí sáruithe, chomh maith le nasc chun na foirme maidir le fógra a thabhairt i ndáil le sárú, ar leathanach an fhógra sáraithe ar láithreán gréasáin an DPC.

Tá dhá phríomhoibleagáid ar rialaitheoirí faoin réimeas nua seo: **(a)** fógra maidir le haon sárú ar shonraí pearsanta a thabhairt *don DPC*, mura bhfuil sé ar chumas an rialaitheora a léiriú nach dóigh go mbeidh riosca do na hábhair sonraí mar thoradh air; agus **(b)** an sárú a chur in iúl do na *hábhair sonraí*, más dóigh go mbeidh ardriosca do na hábhair sonraí i gceist leis. Tá sé fíorthábhachtach go mbeidh tuiscint agus go gcomhlíonfaidh rialaitheoirí an *dá* oibleagáid seo.

Tá príomhoibleagáid eile atá ar rialaitheoirí i gcomhthéacs sárú sonraí pearsanta a thagann chun cinn ón bprionsabal cuntasachta, leagtha amach in Airteagal 5(2) den GDPR, chomh maith leis na ceanglais in Airteagal 33(5). Faoi Airteagal 5(2) den GDPR, tá sé de fhreagracht ar rialaitheoirí a léiriú go bhfuil na prionsabail eile cosanta sonraí á gcomhlíonadh acu, lena n-áirítear, prionsabal 'ionracas agus rúndachta', agus faoi Airteagal 33(5) ní mór do rialaitheoirí doiciméadú a dhéanamh ar an bhfaisnéis ábhartha chun a chur ar chumas an DPC a gcomhlíontacht lena gcuid oibleagáid faoi Airteagal 33 a dhearbhú.

Ní mór do rialaitheoir na sáruithe go léir i ndáil le sonraí pearsanta a thaifeadfadh, lena n-áirítear, na fíricí a bhain leis an sárú i ndáil le sonraí pearsanta, cén uair agus conas a fuair siad amach faoin sárú, tionchair an tsáraithe agus an gníomh/na gníomhartha leasúcháin a glacadh – cuirfidh sé seo ar a gcumas comhlíonadh an réimis fógra maidir le sárú sonraí a léiriú don DPC. Ba chóir go n-áireodh an cháipéisíocht seo mionsonraí maidir leis an mbealach ar thug an rialaitheoir faoi mheasúnú a dhéanamh ar dhóchúlacht riosca agus ar dhéine an riosca ar chearta agus ar shaoirsí an ábhair sonraí.

Cad is sárú i ndáil sonraí pearsanta ann?

Ciallaíonn sárú i ndáil le sonraí pearsanta, sárú slándála a mbíonn scrios trí thionóisc nó neamhdhleathach, cailleadh, athrú, nochtadh neamhúdaraithe ar, nó rochtain chuig

sonraí pearsanta mar thoradh air.[2] Ciallaíonn an téarma 'sonraí pearsanta' a fhaisnéis a bhaineann le duine aonair sainaitheanta nó inaitheanta. Áirítear ar sháruithe sonraí pearsanta, eachtraí a d'fhéadfadh a bheith mar thoradh ar thionóiscí (ar nós ríomhphost a sheoladh chuig an bhfaighteoir mhícheart) chomh maith le gníomhartha d'aon turas, (ar nós ionsaithe fioscaireachta chun rochtain a fháil ar shonraí custaiméara).

Tarlaíonn sárú sonraí pearsanta le linn tionóiscí ina gcaillteár, a scriostar, a dtruaillítear nó a nochtar go neamhdhlisteanach na sonraí pearsanta. Áirítear leis seo, cásanna sa chás go ndéanann duine éigin sonraí a nochtadh nó a gcuirtear na sonraí ar aghaidh gan údarú cuí, nó sa chás nach féidir na sonraí a fháil trí chriptiú le bogearraí éirice, nó na sonraí a chailleadh nó a scrios trí thionóisc.

I mbeagán focal, is ionann sárú sonraí pearsanta agus eachtra slándála a mbíonn tionchar diúltach aige ar rúndacht, ionracas nó fáil a bheith ar shonraí pearsanta; a chiallaíonn nach bhfuil sé ar chumas an rialaitheora comhlíontacht a chinntiú leis na prionsabail a bhaineann le próiseáil sonraí pearsanta mar a leagtar amach in Airteagal 5 den GDPR. Cé gur eachtraí slándála atá i gceist le gach sárú ar shonraí pearsanta, ní gá go mbeadh sárú sonraí pearsanta i gceist le gach eachtra slándála.

Cén uair nach mór do rialaitheoir fógra a thabhairt don DPC maidir le sárú faoin GDPR?

Tá rialaitheoir faoi oibleagáid fógra a thabhairt don DPC maidir le haon sárú sonraí pearsanta a tharlaíonn, *mura* bhfuil ar a gcumas a léiriú *nach dóigh go mbeidh riosca mar thoradh* ar *shárú sonraí pearsanta ó thaobh cearta agus saoirsí daoine nádúrtha*.[3] Ciallaíonn sé seo gurbh é an seasamh réamhshocraithe do rialaitheoirí ná gur chóir dóibh na sáruithe go léir a chur in iúl don DPC, seachas sna cásanna a bhfuil measúnú déanta ag an rialaitheoir ar an sárú agus nach dóigh go mbeidh riosca i gceist do na hábhair sonraí, agus go bhfuil sé ar chumas an rialaitheora léiriú a thabhairt ar an gcúis atá aige/aici le teacht ar an gcinneadh. Ar aon nós, ó thaobh gach sárú – fiú na cinn nach gcuirtear in iúl don DPC, ar an mbonn go meastar nach dóigh go mbeidh riosca mar thoradh orthu – ní mór do rialaitheoir taifead a dhéanamh de mhionsonraí an tsáraithe ar a laghad, an measúnú a bhaineann leis, a thionchar, agus na céimeanna atá glactha mar fhreagra, de réir mar a cheanglaítear le hAirteagal 33(5) den GDPR.

Nuair a fhaigheann rialaitheoir eolas maidir le sárú i ndáil le sonraí pearsanta a bhféadfadh riosca ar bith a bheith mar thoradh ar an sárú do chearta agus do shaoirsí ábhar sonraí, ní mór dóibh fógra a thabhairt don DPC 'gan mhoill mhíchuí', nó 'chomh

[2] Féach Airteagal 4(12) den GDPR chun sainmhíniú a fháil ar 'sárú sonraí pearsanta'.
[3] Féach Réamhaithris 85 agus Airteagal 33(1) den GDPR

luath agus is féidir',[4] agus, nuair is féidir, tráth nach deireanaí ná 72 uair an chloig tar éis don rialaitheoir a fháil amach faoin sárú. Ba chóir a mheas go bhfuil rialaitheoir ar an 'eolas' nuair a bhíonn sé/sí réasúnta cinnte gur tharla eachtra sáraithe agus go bhfuil sonraí pearsanta curtha i mbaol.[5]

Ní mór do rialaitheoirí, ar mhaithe lena gcuid oibleagáidí a chomhlíonadh faoi phrionsabal cuntasachta Airteagal 5(2) chomh maith leis an gceanglas faisnéis ábhartha a thaifeadadh faoi Airteagal 33(5), go mbeidh ar a gcumas a léiriú don DPC cén uair agus conas a fuair siad amach faoin sárú i ndáil le sonraí pearsanta. Molann an DPC, go mbeidh córas i bhfeidhm ag rialaitheoirí, mar chuid dá nósanna imeachta maidir le sárú inmheánach, chun taifeadadh a dhéanamh ar cén uair agus conas a fuair siad amach faoi na sáruithe ar shonraí pearsanta agus cén chaoi a ndearnadh measúnú ar an riosca a d'fhéadfadh an sárú a chruthú.

Má theipeann ar rialaitheoir an DPC a chur ar an eolas laistigh de 72 uair an chloig, ní mór dóibh cúis a thabhairt leis an mhoill chomh maith leis an bhfógra deireanach a thabhairt don DPC agus d'fhéadfadh siad a bheith ag sárú a n-oibleagáid fógra a thabhairt *gan mhoill mhíchuí* – mura mbíonn an chúis a tugadh leordhóthanach le húdar maith a bheith leis an mhoill. Sa chás nach bhfuil sé indéanta an fhaisnéis ábhartha go léir a chur ar fáil don DPC laistigh den tréimhse 7 uaire an chloig, ní mór an fógra tosaigh a lóisteáil agus an fhaisnéis a sholáthar i gcéimeanna ansin, chomh fada agus go ndéantar é sin gan mhoill mhíchuí agus ar an gcoinníoll gur féidir leis an rialaitheoir cúiseanna a thabhairt leis an mhoill de réir Airteagal 33(1).

Maidir le hamlíne ó thaobh fógra a thabhairt, moltar i dtreoirlínte Mheitheal Oibre Airteagal 29, nuair a thugann rialaitheoir fógra maidir leis an sárú i dtús báire, ba chóir an t-údarás maoirseachta a chur ar an eolas nach bhfuil an fhaisnéis go léir atá ag teastáil aige/aici go fóill agus go gcuirfear tuilleadh faisnéise ar fáil níos deireanaí.

Ar an gcaoi chéanna, de réir Airteagal 33(2) den GDPR, ní mór do phróiseálaí sonraí, atá ag próiseáil sonraí pearsanta ar threoir ón rialaitheoir sonraí, fógra a thabhairt dá rialaitheoir sonraí maidir le haon sárú ar shonraí pearsanta gan mhoill mhíchuí tar éis dó/di eolas a fháil faoi shárú. Tá sé seo ríthábhachtach ó thaobh cur ar chumas na rialaitheoirí a gcuid oibleagáidí a chomhlíonadh maidir le fógra. Ní mór na ceanglais seo ar thuairisciú sáruithe a bheith mionsonraithe sa chonradh idir an rialaitheoir agus an próiseálaí, mar a cheanglaítear faoi Airteagal 28 den GDPR.

[4] Treoirlínte Mheitheal Oibre Airteagal 29, leathanach 20
[5] Treoirlínte Mheitheal Oibre Airteagal 29, leathanach 10

Cad ba chóir a bheith i bhfógra chuig an DPC?

Ní mór go mbeidh ar a laghad, i bhfógra ó rialaitheoir maidir le sárú sonraí pearsanta chuig an DPC (is féidir a dhéanamh trí fhoirm maidir le fógra sáraithe ar láithreán gréasáin an DPC):[6]

a) cur síos ar nádúr an tsáraithe ar na sonraí pearsanta, lena n-áirítear, catagóirí agus líon garbh de na hábhair sonraí, atá i gceist, agus catagóirí agus líon garbh de na taifid sonraí pearsanta atá i gceist;

b) ainm agus mionsonraí teagmhála a chur in iúl don oifigeach cosanta sonraí (DPO) nó pointe teagmhála eile san áit is féidir tuilleadh faisnéise a fháil;

c) cur síos ar na hiarmhairtí a d'fhéadfadh a bheith ar shárú sonraí pearsanta; agus

d) cur síos ar bhearta a glacadh nó a moladh chun aghaidh a thabhairt ar shárú sonraí pearsanta, lena n-áirítear, sa chás gur cuí, bearta le maolú a dhéanamh ar thionchair dhochracha a d'fhéadfadh a bheith ann.

Chun cuidiú leis an DPC le measúnú a dhéanamh ar chomhlíonadh an cheanglais fógra a thabhairt 'gan mhoill mhíchuí', chomh maith le prionsabal na cuntasachta, molann an DPC gur chóir go n-áireodh rialaitheoir, ina bhfógra tosaigh, faisnéis maidir le conas agus cén uair a fuair siad amach faoi shárú na sonraí pearsanta, chomh maith le míniú maidir le haon mhoill, más infheidhme.

Mar a luaitear thuas, sa chás, sa mhéid, nach bhfuil sé indéanta an fhaisnéis go léir atá ag teastáil a chur ar fáil ag an am céanna, féadfar an fhaisnéis a chur ar fáil ina céimeanna, chomh fada is nach bhfuil aon mhoill mhíchuí eile i gceist.[7]

Cén uair nach mór do rialaitheoir sárú i ndáil le sonraí pearsanta a chur in iúl d'ábhair sonraí?

Tá sé d'oibleagáid ar rialaitheoir freisin sárú sonraí pearsanta a chur in iúl don ábhar sonraí, 'gan mhoill mhíchuí', sa chás go 'bhféadfadh ardriosca do chearta agus do shaoirsí an duine nádúrtha a bheith mar thoradh' ar an sárú i ndáil le sonraí pearsanta'.[8] Tá an oibleagáid seo sa bhreis agus ar leith ón oibleagáid an DPC a chur ar an eolas maidir le sáruithe i ndáil le sonraí pearsanta, agus leagtar amach tairseach níos airde atá le feidhmiú agus atá chun tosaigh ar an oibleagáid seo an t-ábhar sonraí a chur ar an eolas. Is é an cuspóir atá taobh thiar den cheanglas seo a chinntiú go nglacann na hábhair sonraí

[6] Féach Airteagal 33(3) den GDPR
[7] Féach Airteagal 33(4) den GDPR
[8] Féach Réamhaithris 86 agus Airteagal 34(1) den GDPR

na réamhchúraimí riachtanacha sa chás gur tharla eachtraí a bhféadfadh ardriosca a bheith ag gabháil leo.

Ní mór faisnéis den sórt sin a thabhairt do na hábhair sonraí gan mhoill, sa chás gur chuí, i gcomhoibriú dlúth leis an DPC, agus de réir na treorach a chuireann an DPC nó údaráis ábhartha eile ar fáil ar nós údaráis forfheidhmithe dlí. I gcásanna ina bhfuil gá leis an riosca láithreach do na hábhair sonraí a mhaolú, beidh sé riachtanach cumarsáid phras a dhéanamh leis na hábhair sonraí.

Tá imthosca ann, mar sin féin, go bhféadfadh sé nár ghá do rialaitheoirí faisnéis maidir le sárú sonraí pearsanta a thabhairt do na hábhair sonraí, fiú má d'fhéadfadh ardriosca ar chearta agus ar shaoirsí an duine nádúrtha a bheith mar thoradh air. Ciallaíonn na himthosca seo, an cás go bhfreastalaítear ar aon cheann de na coinníollacha seo a leanas:[9]

a) tá na bearta cosanta teicniúla agus eagraíochtúla cuí curtha i bhfeidhm ag an rialaitheoir, agus cuireadh na bearta seo i bhfeidhm ar na sonraí pearsanta a bhí faoi thionchar ag an sárú i ndáil le sonraí pearsanta, go háirithe bearta a dhéanann na sonraí pearsanta dothuigthe do dhuine ar bith nach bhfuil údaraithe lena rochtain, ar nós criptiú;

b) ghlac an rialaitheoir céimeanna ina dhiaidh sin lena chinntiú nach dóigh go dtiocfaidh ardriosca i leith cearta agus saoirsí na n-ábhar sonraí chun cinn níos mó; nó

c) bheadh iarracht díréireach i gceist. I gcás den sórt sin, áfach, ní mór do rialaitheoir fós a chinntiú, trí chumarsáid phoiblí nó trí bheart eile go bhfuil ábhair sonraí ar an eolas ar bhealach atá chomh héifeachtach céanna.

Cad ba chóir a bheith i gcumarsáid chuig an ábhar sonraí?

Ba chóir go ndéanfadh an chumarsáid maidir le sárú sonraí pearsanta don ábhar/do na hábhair sonraí, cur síos ar nádúr an tsáraithe i ndáil le sonraí pearsanta chomh maith le moltaí don ábhar sonraí atá i gceist leis na tionchair dhochracha a d'fhéadfadh a bheith ar an sárú a mhaolú.

Ní mór go ndéanfaidh an chumarsáid seo chuig an ábhar sonraí cur síos i dteanga atá soiléir agus simplí ar nádúr an tsáraithe i ndáil le sonraí pearsanta agus ba chóir go n-áireodh sé seo an fhaisnéis seo a leanas ar a laghad (mar a cheanglaítear le hAirteagal 34(2) den GDPR):

[9] Féach Airteagal 34(3) den GDPR

- ainm agus mionsonraí teagmhála an oifigigh cosanta sonraí nó pointe teagmhála eile inar féidir tuilleadh eolais a fháil;
- cur síos ar na hiarmhairtí a d'fhéadfadh a bheith ag sárú i ndáil le sonraí pearsanta; agus
- cur síos ar na bearta atá glactha nó molta ag an rialaitheoir a glacadh chun aghaidh a thabhairt ar an sárú i ndáil le sonraí pearsanta, lena n-áirítear, bearta le tionchair dhochracha a mhaolú.

Ar féidir le rialaitheoirí ábhair sonraí a chur ar an eolas fiú mura meastar go mbíonn an riosca ard?

Cé nach bhfuil aon oibleagáid ar rialaitheoirí sonraí sárú i ndáil le sonraí pearsana a chur in iúl do na hábhair sonraí atá faoi thionchar ag an sárú, murar dóigh go mbeidh ardriosca ann dóibh, mar sin féin, tá saor chead ag rialaitheoirí sárú a chur in iúl do na hábhair sonraí sa chás go rachaidh sé chun leasa nó go mbeidh sé cuí dóibh a leithéid a dhéanamh, i gcomhthéacs an tsáraithe áirithe sin.

Measúnú Riosca

Baineann ceann de na príomhréimsí lenar ardaigh rialaitheoirí fiosrúcháin leis an DPC le measúnú riosca. Mar go mbaineann measúnú ar an fhéidearthacht nó ar an riosca a d'fhéadfadh sárú a chruthú leis an dá thairseach **(a)** an tairseach maidir le fógra a thabhairt don DPC, agus **(b)** an tairseach lena chur in iúl don ábhar sonraí gur tharla sárú, d'fhéadfadh mainneachtain measúnú leordhóthanach a dhéanamh ar riosca (nó gan iarracht ar bith a dhéanamh le measúnú a dhéanamh ar riosca), go bhféadfadh sé go gclisfeadh ar na rialaitheoirí freastal ar a gcuid oibleagáidí faoin GDPR mar thoradh air.

I roinnt cásanna, rinne rialaitheoirí, sna fógraí i ndáil le sárú a thug siad don DPC, rátáil ar an riosca do chearta agus do shaoirse an ábhair/na n-ábhar sonraí, a bheith níos ísle ná mar a bhíothas ag súil leis, ag tógáil nádúr na sáruithe a bhí i gceist san áireamh. D'fhéadfadh sé nach gcuirfeadh rialaitheoirí béim leordhóthanach ar chritéar áirithe agus iad i mbun measúnaithe ar dhóchúlacht agus ar chomh tromchúiseach is atá riosca a d'fhéadfadh a bheith ann do na hábhair sonraí. Áirítear ar fhachtóirí ba chóir do rialaitheoirí a thabhairt san áireamh agus iad bainteach le measúnú den sórt sin, ach níl siad teoranta do:

- cineál agus nádúr na sonraí pearsanta (lena n-áirítear cibé an áiríonn sé sonraí pearsanta atá íogair nó ar 'catagóir speisialta' iad);
- imthosca an tsáraithe i ndáil le sonraí pearsanta;
- cibé an bhfuil nó nach bhfuil sonraí pearsanta cosanta trí bhearta cosanta teicniúla cuí, ar nós criptiú nó na sonraí a dhéanamh anaithnid;
- éascaíocht sainaithint dhíreach nó indíreach na n-ábhar sonraí atá faoi thionchar;
- dóchúlacht aisiompú bréagainmniú nó cailliúint rúndachta;
- dóchúlacht calaois aitheantais, caillteanas airgid, nó cineálacha eile mí-úsáide sonraí pearsanta;
- cibé an bhféadfaí sonraí pearsanta a úsáid go mailíseach;
- an dóchúlacht go bhféadfadh an sárú a bheith mar thoradh air, agus déine an damáiste fisiciúil, ábhartha nó neamhábhartha do na hábhair sonraí; agus
- cibé an bhféadfadh idirdhealú, damáiste do chlú nó damáiste do chearta bunúsacha eile na n-ábhar sonraí, a bheith mar thoradh ar an sárú.

Sá chás go dteipeann ar rialaitheoirí na critéir ábhartha go léir maidir le measúnú riosca a d'fhéadfadh a bheith ann do na hábhair sonraí a bhreithniú, nó béim leordhóthanach a chur orthu, d'fhéadfadh sé go mbeadh 'tearcthuairisciú' mar thoradh air sin – mainneachtain fógra a thabhairt don DPC maidir le sárú sonraí sá chás fógra a bheith

riachtanach. Ní mór do rialaitheoirí a thabhairt ar aird nach mór dóibh fógra a thabhairt don DPC maidir le sárú sonraí pearsanta, mura bhfuil ar a gcumas a léiriú nach dóigh go mbeidh riosca i gceist do chearta ná do shaoirsí na n-ábhar sonraí.

Ar an lámh eile, i líon beag de chásanna, tugadh faoi dearadh gur thuairiscigh rialaitheoirí sáruithe sonraí nach raibh *aon riosca* i gceist leo do na hábhair sonraí, a raibh 'ró-thuairisciú' i gceist leo i roinnt cásanna.

Tá sé tábhachtach ar an bpointe is a fhaigheann rialaitheoirí amach faoi shárú sonraí pearsanta, chomh maith le hiarracht a dhéanamh an eachtra a choinneáil faoi smacht, tabhairt faoi mheasúnú ar an riosca a d'fhéadfadh a bheith ann mar thoradh air. Faoi Airteagal 33 den GDPR, níl aon fhógra riachtanach má mheastar '*nach dóigh go mbeidh riosca i gceist*' do chearta agus do shaoirsí na n-ábhar sonraí. Ní mór tabhairt faoin measúnú riosca seo agus doiciméadú a dhéanamh ar an riosca i gcás sáruithe sonraí pearsanta.

Nuair a dhéantar measúnú nach dóigh go mbeidh riosca mar thoradh ar shárú sonraí pearsanta do na hábhair sonraí, ansin, ar an dara measúnú agus measúnú ar leith ar chóir don rialaitheoir tabhairt faoi ná cíbe an bhfuil nó nach bhfuil riosca ann agus go bhfuil an rialaitheoir faoi oibleagáid freisin é sin a chur in iúl d'ábhair sonraí a bhféadfadh tionchar a bheith orthu.

Tá na mionsonraí maidir leis an méid ba chóir a chur in iúl ar fáil thuas, faoin gceannteideal '*Cén uair nach mór do rialaitheoir sárú i ndáil le sonraí pearsanta a chur in iúl do na hábhair sonraí?*', ach tá feidhm leis an treoir chéanna maidir le measúnú – ní mór do rialaitheoirí na critéir ábhartha go léir a thógáil san áireamh nuair atáthar i mbun measúnaithe ar cibé an *'bhféadfadh ardriosca do chearta agus do shaoirsí an duine nádúrtha*' a bheith mar thoradh ar an sárú agus ba chóir taifead a choinneáil ar cén chaoi agus cén uair a rinneadh an measúnú seo.

Moltar do rialaitheoirí, chun comhlíonadh a gcuid oibleagáidí a léiriú, taifead a choinneáil ar cén chaoi agus cén uair a rinneadh na measúnuithe.

Le tuilleadh faisnéise a fháil conas measúnú a dhéanamh ar riosca i gcomhthéacs sárú sonraí pearsanta, molann an DPC go rachaidh rialaitheoirí i gcomhairle le hAlt IV, 'Measúnú a Dhéanamh ar Riosca agus ar Ardriosca', Mheitheal Oibre Airteagal 29 'Treoirlínte maidir le fógra i ndáil le sárú sonraí pearsanta'.

Cás-Staidear – Gannmheas Riosca

Daoine Soghonta is Ábhar do na Sonraí

Chuir rialaitheoir an DPC ar an eolas maidir le sárú a d'fhéadfadh a bheith déanta ar sholáthróir cúram sláinte a bhí thíos le hionsaí bogearraí éirice. Tugadh breac-chuntas go ndearnadh ionsaí agus criptiú ar an gcóras saotharlainne agus ar chóras cúltaca na saotharlainne a chiallaigh gur cuireadh i mbaol iad. Sonraíodh go bhféadfadh tionchar a bheith ag an ionsaí ar shonraí ar thart ar 50,000 duine is ábhar do na sonraí.

Léirigh an rialaitheoir, san fhógra a thug an rialaitheoir don DPC nach raibh riosca 'ardleibhéil' i gceist leis do na sonraí.

Mar sin féin, tar éis anailís a rinne Aonad Measúnaithe Sáraithe an DPC ar an bhfógra tosaigh agus athbhreithniú ar na doiciméid a chuir an rialaitheoir ar fáil agus i bhfianaise na gcatagóirí de shonraí pearsanta a d'fhéadfadh a bheith faoi thionchar, agus soghontacht na n-ábhar sonraí, rinne an DPC cinneadh gur 'dóigh go mbeidh ardriosca i gceist do chearta agus do shaoirsí na n-ábhar sonraí'.

Ní amháin go raibh gá an sárú a chur in iúl don DPC, ach, mar gheall ar an ardriosca a bhí i gceist, bheadh gá le teagmháil a dhéanamh leis na hábhair sonraí a bhí faoi thionchar ag an ionsaí.

Sárú a raibh Calaois mar Thoradh air

Chuir rialaitheoir an DPC ar an eolas go raibh rochtain neamhúdaraithe faighte ag tríú páirtí chuig cuntas ríomhphoist fostaí de bharr eachtra fioscaireachta/haiceáil.

Mar thoradh ar an eachtra sin, bhí ábhar sonraí amháin thíos le calaois airgeadais. Dá bhrí sin, léirigh an rialaitheoir, san fhógra chuig an DPC, go raibh leibhéal an riosca do na hábhair sonraí 'Íseal'.

Mar sin féin tar éis anailís a rinne Aonad Measúnaithe Sáraithe an DPC ar an bhfógra tosaigh agus athbhreithniú ar na doiciméid a chuir an rialaitheoir ar fáil agus go háirithe i bhfianaise nádúr na sonraí pearsanta a bhí faoi thionchar, agus an fhíric go raibh díobháil i ndáiríre déanta don ábhar sonraí, rinneadh cinneadh gur 'dóigh go mbeidh ardriosca i gceist do chearta agus do shaoirsí na n-ábhar sonraí'.

Ní amháin go raibh gá an sárú a chur in iúl don DPC, ach, mar gheall ar an ardriosca a bhain leis, b'éigin teagmháil a dhéanamh leis na hábhair sonraí a bhí faoi thionchar ag an ionsaí.

Cás-Staidear – Rómheas Riosca

Gan aon Riosca Inaitheanta ann

Chuir rialaitheoir sonraí áirithe, ar líon ócáidí, fógraí i ndáil le sárú sonraí pearsanta faoi bhráid lenar bhain cáipéisí tacaíochta a scanadh isteach ar a gcóras ach á sábháladh ina dhiaidh sin chuig fillteán leictreonach mícheart an ábhair sonraí.

Coinníodh, níor athraíodh agus níor nochtadh na sonraí pearsanta le haon pháirtithe neamhúdaraithe agus nuair a braitheadh an earráid cuireadh na sonraí pearsanta isteach sa bhfillteán leictreonach ceart – ní dóigh, dá bhrí sin, go mbeidh riosca i gceist don ábhar sonraí.

Tar éis athbhreithniú a dhéanamh ar na heachtraí seo, thángthas ar an gcinneadh nach raibh fógra riachtanach faoi Airteagal 33(1) den GDPR, ar an mbonn nach raibh aon riosca inaitheanta i gceist, agus 'ní dóigh go mbeadh na heachtraí ina riosca do chearta ná do shaoirsí daoine nádúrtha'.

Faighteoirí Iontaofa

Bhí an coincheap 'faighteoirí iontaofa' i líon fógraí a chuir rialaitheoirí faoi bhráid an DPC. Féadfaidh rialaitheoir, nuair a bhíonn siad i mbun measúnaithe ar riosca a d'fhéadfadh sárú i ndáil le sonraí pearsanta a chruthú, agus ag brath ar na himthosca, mar chuid dá mheasúnú/dá measúnú, breithniú a dhéanamh cibé a bhfuil faighteoir 'iontaofa'.

D'fhéadfadh an rialaitheoir a theacht ar an gconclúid go bhfuil an faighteoir iontaofa nuair a bhíonn caidreamh leanúnach ag an rialaitheoir leis an bhfaighteoir agus go bhféadfaí a mheas go bhféadfadh údarás a bheith aige/aici le sonraí pearsanta a phróiseáil, go bhfuil eolas ag an bhfaighteoir ar na nósanna imeachta agus ar an stair atá i gceist, agus go bhfuil leibhéal leordhóthanach muiníne ag an rialaitheoir nach ndéanfaidh an faighteoir sonraí a rochtain nó a léamh agus go mbeidh treoracha an rialaitheora á gcomhlíonadh acu leis na sonraí a choinneáil slán, ag maolú an tsáraithe ar an mbealach sin agus ag ísliú déine an riosca.

In imthosca áirithe, atá thar a bheith teoranta, d'fhéadfadh rannpháirtíocht faighteora iontaofa an dóchúlacht ó thaobh riosca do na hábhair sonraí a ísliú a mhéid is go mbeifí in ann fáil réidh leis an riachtanas fógra i ndáil le sárú sonraí pearsanta a thabhairt don DPC. I gcás ar bith, ní mór don rialaitheoir na heachtraí a thaifeadadh i gcónaí sna logleabhair inmheánacha.

Ní dóigh go dtiocfadh fáil réidh le riosca *ar bith* ar chearta nó ar shaoirsí an ábhair sonraí, a chuireann deireadh ar an mbealach sin leis an riachtanas fógra a thabhairt don DPC, chun cinn ach in imthosca atá thar a bheith teoranta, ar nós, sa chás go ndearnadh sonraí pearsanta a nochtadh le faighteoir a bhí údaraithe go cothrom le sonraí pearsanta a fháil, ar nós comhalta foirne laistigh den aonad céanna leis an duine aonair a rinne an nochtadh.

Cibé an faighteoir iontaofa atá i bhfaighteoir na sonraí pearsanta nó nach ea, d'fhéadfadh sé a bheith ábhartha, mar sin féin, sa mheasúnú cibé ar gá dul i dteagmháil leis na hábhair sonraí atá faoi thionchar. Beidh oibleagáid ar an rialaitheoir, in go leor cásanna lena bhfuil baint ag faighteoirí iontaofa, an DPC fós a chur ar an eolas maidir le sárú i ndáil le sonraí pearsanta, d'fhéadfadh sé mar geall gur faighteoir iontaofa a bhí sa bhfaighteoir (a bhféadfadh comhaontú a bheith déanta aige/aici, mar shampla, gan na sonraí pearsanta a rochtain) go laghdófaí déine an riosca do na hábhair sonraí agus mar sin nach '*dóigh go mbeidh riosca do chearta agus do shaoirsí na n-ábhar sonraí mar thoradh air*' agus mar sin nach mbeidh cumarsáid éigeantach leis na hábhair sonraí faoi Airteagal 34 den GDPR mar thoradh air.

Tá sé tábhachtach an cheist maidir le cibé an bhfuil faighteoir 'iontaofa' a thabhairt ar aird, agus cén tionchar a d'fhéadfadh a bheith aige sin (má bhíonn a leithéid i gceist) ar

dhóchúlacht nó ar dhéine an riosca a chruthaíonn sárú sonraí pearsanta, ag brath ar imthosca gach aon chás agus ní mór measúnú a dhéanamh ar gach eachtra ar bhonn cás ar chás.

Fógra Deireanach nó Gan aon Fhógra a Thabhairt

Sa chás, mar a thugtar aghaidh air thuas, faoin gceannteideal '*Measúnú Riosca*', go bhfuil míthuiscint ar rialaitheoirí maidir leis an tairseach i ndáil le fógra nó le cumarsáid sárú sonraí pearsanta, nó fiú má theipeann orthu go hiomlán measúnú riosca a dhéanamh maidir leis an sárú sin, is minic a tharla sé nár tugadh aon fhógra don DPC nó nár cuireadh na n-ábhar sonraí ar an eolas maidir leis an sárú, agus fógra dá leithéid sin riachtanach. Chomh maith leis sin, i líon cásanna, thug rialaitheoirí fógra don DPC maidir le sárú i ndáil le sonraí pearsanta, ach níor cuireadh é sin i gcrích laistigh den teorainn ama chuí agus níor cuireadh údar leordhóthanach ar fáil ó thaobh fógra deireanach a thabhairt.

Ní mór do rialaitheoirí a thabhairt ar aird nach mór na ceanglais le fógra a thabhairt nó le cumarsáid a dhéanamh i ndáil le sárú sonraí pearsanta a chomhlíonadh '*gan mhoill mhíchuí*', agus ní mór údar maith a bheith le haon mhoill ó thaobh fógra nó cumarsáid. Mar a leagtar amach thuas, beidh baint aige seo freisin sa chás nach mbíonn rialaitheoir in ann an fhaisnéis go léir a sholáthar don DPC laistigh de na chéad 72 uair an chloig.

Ní mór do rialaitheoir ar bith a thugann patrún ó thaobh a bheith deireanach faoi deara ina bhfógra, breithniú leasú a dhéanamh ar an mbeartas agus ar a nósanna imeachta i ndáil le fógra sáraithe, ag cinntiú go bhfuil cúis mhaith le haon mhoill ó thaobh fógraí agus breithniú a dhéanamh cibé ar chóir an fhaisnéis a chur ar fáil i gcéimeanna sa chás nach mbíonn fógra iomlán indéanta láithreach bonn.

Mar a thugtar ar aird thuas, ar mhaithe le comhlíonadh cheanglais an GDPR a léiriú, go háirithe na ceanglais fógra a thabhairt don DPC nó cumarsáid a dhéanamh leis na hábhair sonraí '*gan mhoill mhíchuí*', ba chóir do rialaitheoir taifead a choinneáil maidir le conas agus cén uair a fuair siad amach den chéad uair faoin sárú i ndáil le sonraí pearsanta.

Cás-Staidéar– Gan aon Chumarsáid

Gan cumarsáid a dhéanamh leis na hÁbhair Sonraí

Thug comhlacht poiblí fógra don DPC maidir le sárú lena raibh eachtra cibearshlándála ar a láithreán gréasáin i gceist. Mar gheall ar nádúr na seirbhísí a chuireann an comhlacht poiblí ar fáil trína láithreán gréasáin agus an eachtra slándála a braitheadh, bhí an fhéidearthacht ann go mbeadh lear mór sonraí pearsanta á nochtadh.

Rinne an rialaitheoir measúnú ar an riosca do na hábhair sonraí mar riosca 'Íseal'. Tar éis anailís a rinne Aonad Measúnaithe Sáraithe an DPC, áfach, agus tar éis athbhreithniú a dhéanamh ar

na cáipéisí tacaíochta agus i bhfianaise na gcatagóirí de shonraí pearsanta a d'fhéadfadh a bheith faoi thionchar, an tionchar a bhíonn ag an tuairisciú ar na hábhair sonraí, agus na gníomhartha/bearta ar tugadh fúthu, rinneadh cinneadh 'gur dóigh go mbeidh riosca ard do chearta agus do shaoirsí na n-ábhar sonraí mar thoradh air' agus ní raibh feidhm le ceachtar de na heisceachtaí faoi Airteagal 34(3).

Sa chás seo, chlis ar an rialaitheoir measúnú leordhóthanach a dhéanamh ar an riosca a d'fhéadfadh a bheith i gceist do na hábhair sonraí agus dá bhrí sin theip air/uirthi cumarsáid a dhéanamh leis na hábhair sonraí a bhí faoi thionchar, mar a cheanglaítear faoi Airteagal 34 den GDPR, agus tugadh treoir dó/di ina dhiaidh sin an chumarsáid a bhí riachtanach a dhéanamh.

Tuairisciú nach bhfuil Leordhóthanach

I roinnt cásanna, aithníodh nach raibh faisnéis leordhóthanach maidir le heachtraí sáruithe sonraí pearsanta a bhí braite acu á chur ar fáil ag rialaitheoirí d'Aonad Measúnaithe Sáraithe an DPC. D'fhéadfadh faisnéis easnamhach a bheith i gceist nuair a chuireann rialaitheoirí fógraí neamhiomlána ar fáil, nuair a fhágtar faisnéis ábhartha amach nó má chlistear ó thaobh measúnuithe riosca leordhóthanacha a thabhairt chun críche. D'fhéadfadh moill shuntasach a bheith i gceist leis seo agus d'fhéadfadh, i roinnt cásanna, cliseadh ó thaobh an rialaitheora a chuid/a cuid oibleagáidí a chomhlíonadh, sé sin faisnéis a sholáthar mar a cheanglaítear faoi Airteagal 33(3) den GDPR.

Ní mór do rialaitheoirí a chinntiú, trína mbeartais agus a nósanna imeachta féin, go gcuirtear, agus iad ag líonadh isteach foirm maidir le fógra a thabhairt i ndáil le sárú ar líne an DPC, go gcuirtear an fhaisnéis ábhartha go léir atá riachtanach maidir le sárú i ndáil le sonraí pearsanta ar fáil don DPC – ag an gcéim fógartha tosaigh agus nuair atáthar ag tabhairt uasdátaithe ina dhiaidh sin, más infheidhme.

Ba chóir do rialaitheoir iarracht a dhéanamh, ar a laghad ar bith, an fhaisnéis go léir atá luaite in Airteagal 33(3) den GDPR agus atá pléite faoin gceannteideal '*Cad ba chóir a bheith i bhfógra chuig an DPC?*' thuas, a chur san áireamh.

Ar an gcaoi chéanna, sa chás go bhfuil sé cuí a leithéid a dhéanamh, ba chóir do rialaitheoirí a chinntiú freisin agus iad ag cur sárú maidir le sonraí pearsanta in iúl do na hábhair sonraí, go gcuireann siad an fhaisnéis go léir atá riachtanach ar fáil do na hábhair sonraí, lena n-áirítear, ar a laghad, an fhaisnéis atá liostaithe faoin gceannteideal *'Cad ba chóir a bheith i gcumarsáid leis an ábhar sonraí?* agus in Airteagal 34(2) den GDPR.

Cás-Staidéar– Tuairisciú nach bhfuil Leordhóthanach

Faisnéis atá ar Iarraidh

D'aithin Aonad Measúnaithe Sáraithe an DPC bacainní áirithe ó thaobh próiseála agus meastóireachta fógraí a fuarthas ó chomhlachtaí poiblí áirithe, nuair a bhí faisnéis theoranta

maidir leis an sárú féin sna fógraí tosaigh, an bealach inar tharla an sárú agus na catagóirí sonraí a bhí faoi thionchar.

Thóg iarratais leantacha ar thuilleadh faisnéise go leor ama i roinnt cásanna. Is minic gur tugadh imscrúdú breise ar na heachtraí mar chúiseanna leis an mhoill.

I gcásanna mar iad sin, is é an cur chuige ceart ná uasdátú eatramhach a thabhairt don DPC, agus an méid faisnéise ábhartha is féidir a sholáthar don DPC '*gan mhoill mhíchuí*', seachas gan faisnéis ar bith nó faisnéis theoranta a chur ar fáil nó go n-éilítear go soiléir a leithéid.

Faisnéis Theicniúil

Baineann ceann de na bacainní is minice atá tugtha ar aird ag an DPC san idirghníomhaíocht atá aige le rialaitheoir i gcomhthéacs fógraí i ndáil le sárú sonraí pearsanta leis an leibhéal faisnéise teicniúla atá ag rialaitheoir. Ní mór do rialaitheoirí a chinntiú go mbeidh leibhéal cuí faisnéise teicniúla ar fáil dóibh ar mhaithe lena chur ar a gcumas an fhaisnéis sin a aithint, gan mhoill mhíchuí:

a) go raibh siad thíos le heachtra slándála, ar nós cibear-ionsaí;
b) na bearta agus na gníomhartha nach mór a ghlacadh láithreach tar éis sárú den chineál seo tarlú; agus
c) na cosaintí cuí ba chóir a bheith in úsáid leis an riosca a bhaineann le heachtraí den sórt seo tarlú a laghdú.

Baineann an tsaincheist seo go háirithe le rialaitheoirí beaga go meánmhéide, nach bhfuil acu ach rochtain theoranta ar acmhainní agus ar fhaisnéis i dtéarmaí IT.

Faoin bprionsabal 'ionracas agus cuntasacht' (ceann de na príomhphrionsabail cosanta sonraí atá le fáil in Airteagal 5 den GDPR), is ceanglas é nach mór do rialaitheoirí, agus úsáid á bhaint as bearta teicniúla nó eagraíochtúla cuí, sonraí pearsanta a phróiseáil ar bhealach a chinntíonn slándáil chuí na sonraí, lena n-áirítear, cosaint i gcoinne próiseáil neamhúdaraithe nó neamhdhleathach agus i gcoinne cailleadh, scriosadh nó damáiste de thionóisc. Ciallóidh comhlíonadh an cheanglais seo go gcosnófar na sonraí pearsanta agus go gcuideofar leis an rialaitheoir araon lena fháil amach go tapa cibé ar tharla sárú i ndáil le sonraí pearsanta agus fógra a thabhairt don DPC go scafánta.

Leis an méid sin a bhaint amach, ní mór do rialaitheoirí bearta iomchuí teicniúla nó eagraíochtúla a úsáid. Sa chás nach bhfuil an leibhéal atá riachtanach d'eolas teicniúil ag na rialaitheoirí iad féin, ní mór dóibh an oiliúint chuí nó comhairle sheachtrach nó tacaíocht ICT a lorg.

Cás-Staidéar – Faisnéis Theicniúil nach bhfuil Leordhóthanach

Neamhábaltacht Soghontacht a Aithint

De bhun fógra a thabhairt don saoránach atá i gceist, rinne Aonad Measúnaithe Sáraithe an DPC teagmháil le rialaitheoir maidir le custaiméirí a bhí ag fáil ríomhphost turscair a raibh an chuma orthu go raibh siad ag teacht ón rialaitheoir. Bhí an chosúlacht air nach raibh an rialaitheoir ar an eolas maidir leis an sárú féideartha a tharla ar an mbonneagar IT agus a raibh ríomhphoist turscair á seoladh gan údarás ón rialaitheoir mar thoradh air.

Ina dhiaidh sin, chuir an rialaitheoir na custaiméirí ar an eolas trí úsáid a bhaint as láithreacht ar na meáin shóisialta. Bhí deacracht ag an rialaitheoir, áfach, foinse an tsáraithe a aithint agus ó thaobh a chinntiú gur tugadh bearta teicniúla cuí isteach leis an riosca a bhain le heachtraí den sórt sin tarlú arís a laghdú.

Ní mór do rialaitheoirí leibhéal faisnéise teicniúla a chinntiú, cibé trí shaineolas inmheánach nó seachtrach, chun cur ar a gcumas bagairtí slándála a d'fhéadfadh tarlú a aithint, na bagairtí a mhaolú agus cosc a chur orthu tarlú amach anseo.

Fógraí Sáraithe a Dhéanamh arís is arís eile

Tá sé tugtha ar aird ag an DPC, i gcás rialaitheoirí áirithe, patrún trína mbraitheann an rialaitheoir céanna an chatagóir sáraithe sonraí céanna ar líon ócáidí. Baineann údar imní áirithe le patrún leantach de sháruithe i ndáil le sonraí pearsanta, go háirithe mar gheall go bhfuiltear ag leanúint leis na sáruithe thar thréimhse fhada agus nuair a léiríonn siad go bhfuil bearta teicniúla agus eagraíochtúla nach bhfuil leordhóthanach i bhfeidhm ag an rialaitheoir le go dtarlódh na sáruithe arís a chosc.

Sa chás go dtagann patrúin mar sin chun cinn, tá sé tábhachtach, go háirithe, go nglacann rialaitheoirí céimeanna lena mbeartas agus a bhfaisnéis theicniúil a fheabhsú agus/nó tacaíocht a fháil ó shaineolaí le soghontacht a mhaolú.

Cás-Staidéar – Fógraí Sáraithe a Dhéanamh arís is arís eile

Cliseadh Maolú a dhéanamh arís agus arís eile

Thuairiscigh rialaitheoir amháin seacht gcinn (7) d'eachtraí don DPC, tráth a bhféadfadh sé gur cuireadh cuntais ríomhphoist chomhaltaí foirne i mbaol. Bhí lear suntasach sonraí pearsanta i gceist, le leibhéil éagsúla riosca do na hábhair sonraí.

Bhí na sáruithe seo, go háirithe mar go raibh siad ag tarlú arís is arís eile, mar thoradh ar chliseadh an rialaitheora na bearta iomchuí teicniúla agus eagraíochtúla a bheith i bhfeidhm aige/aici le slándáil sonraí pearsanta a bhí stóráilte laistigh dá dtimpeallacht IT a chinntiú.

Innealtóireacht Shóisialta

Aithníodh rialaitheoirí áirithe, go háirithe laistigh d'earnáil na teileachumarsáide, mar a bheith thar a bheith soghonta ó thaobh eachtraí 'innealtóireacht shóisialta' a bhfuil rochtain neamhúdaraithe chuig cuntas cumarsáide na n-ábhar sonraí mar thoradh orthu, agus, i roinnt cásanna, a bhfuil na hábhair sonraí seo faoi réir ag calaois.

Is réimse eile atá i gceist anseo a bhfuil faisnéis theicniúil leordhóthanach agus bearta teicniúla agus eagraíochtúla ríthábhachtach a choinneáil cothrom le dáta leis an tírdhreach teicneolaíochta agus riosca atá ag teacht chun cinn.

Cás-Staidéar – Innealtóireacht Shóisialta

Eachtraí Fioscaireachta a tharlaíonn arís is arís eile

Thuairiscigh rialaitheoir amháin go leor eachtraí lena raibh baint ag innealtóireacht shóisialta, tráth a ndearna déantóir na coire teagmháil leis an rialaitheoir chun tús a chur le hathrú SIM,

agus úsáid a bhaint as mionsonraí dlisteanacha custaiméara chun dul tríd an bpróiseas bailíochtaithe agus smacht a fháil ar chuntas dlisteanach an chustaiméara ar deireadh.

Sa sampla seo, d'fhéadfadh laghdú a bheith déanta ag próiseas bailíochtaithe a bheadh níos láidre ar an bhféidearthacht do rialaitheoirí agus dá gcustaiméirí eachtraí den sórt sin a bhrath.

Cruinneas Sonraí

Baineann 'nochtadh neamhúdaraithe' sonraí pearsanta custaiméirí leis an gcineál sáraithe i ndáil le sonraí pearsanta is coitianta, go háirithe, i dtionscail a bhíonn ag láimhseáil líon mór ríomhphoist nó cumarsáid tríd an bpost, mar gheall nach bhfuil cruinneas na sonraí leordhóthanach ó thaobh taifeadadh a dhéanamh ar shonraí teagmhála.

Is féidir formhór na gcásanna seo a sheachaint má ghlacann rialaitheoirí na céimeanna bunúsacha, ar nós a chinntiú go mbíonn sonraí custaiméirí cruinn agus cothrom le dáta, agus trí mheicníochtaí athbhreithnithe cuí a bheith i bhfeidhm chun comhfhreagras a sheiceáil sula n-eisítear é.

Cé go bhféadfadh earráid atá thar a bheith simplí a bheith mar chúis le sonraí pearsanta duine aonair a sheoladh chuig an bhfaighteoir mícheart, d'fhéadfadh na torthaí do na hábhair sonraí atá faoi thionchar ag nochtadh neamhúdaraithe den sórt seo a bheith tromchúiseach.

Chomh maith leis sin, d'fhéadfadh sé gur léiriú atá sna himthosca a mbíonn eachtraí den sórt sin mar thoradh orthu nach bhfuil bearta teicniúla agus eagraíochtúla leordhóthanacha i bhfeidhm ag rialaitheoirí le slándáil agus le hionracas na sonraí pearsanta atá faoina smacht a chosaint.

Cás-Staidéar – Cruinneas Sonraí

Sonraí Teagmhála Míchearta

Tá líon suntasach sáruithe i ndáil le sonraí pearsanta tuairiscithe ag institiúidí móra airgeadais mar gheall ar thaifeadadh a bheith déanta ar shonraí pearsanta atá mícheart. Áirítear ar na sáruithe seo, taifid chustaiméirí atá mícheart á gcur i gceangal le comhfhreagras atá á sheoladh amach.

Mar thoradh air sin, d'fhéadfadh sonraí pearsanta atá i ráitis bhainc, faisnéis maidir le morgáistí, faisnéis maidir le hiasachtaí, cártaí íocaíochta agus polasaithe árachais a bheith á nochtadh go mícheart.

Is féidir sáruithe den sórt seo a laghdú, nó fáil réidh ar fad leo, trí chéimeanna a ghlacadh lena chinntiú go bhfuil sonraí custaiméirí cothrom le dáta agus go bhfuil meicníochtaí agus nósanna imeachta i bhfeidhm le hathbhreithniú a dhéanamh ar an gcomhfhreagras sula n-eisítear é.

In earnálacha áirithe, tá sáruithe i ndáil le sonraí pearsanta den sórt seo taobh thiar d'fhormhór na sáruithe a thugtar ar aird an DPC. D'fhéadfadh na céimeanna cuí a ghlacadh laghdú

suntasach a dhéanamh ar líon na sáruithe sonraí sna hearnálacha seo a mbíonn tionchar acu ar rialaitheoirí sonraí agus ar na hábhair sonraí.

Conclúidí agus Moltaí

Agus aird á thabhairt ar thaithí Aonad Measúnaithe Sáraithe an DPC, as na staitisticí atá bailithe go dtí seo i ndáil le fógraí sáruithe faoi réimeas fógartha éigeandála an GDPR, agus roinnt de na príomhshaincheisteanna a bhfuil breac-chuntas tugtha ina leith thuas, tá líon breithnithe tábhachtacha nach mór do rialaitheoirí aird a thabhairt orthu agus iad ag déileáil le sáruithe i ndáil le sonraí pearsanta. Leagtar amach thíos achoimre ar na príomhphointí:

Oibleagáidí ó thaobh Fógra a Thabhairt agus Cumarsáid a Dhéanamh – Airteagail 33 agus 34

Ní mór do rialaitheoirí a chinntiú go bhfuil tuiscint acu, agus é sin a léiriú ina gcuid beartas agus nósanna imeachta, go bhfuil dhá phríomhoibleagáid soiléire i gceist, le tástálacha difriúla, i gcomhthéacs réimeas fógartha an GDPR ó thaobh sáruithe i ndáil le sonraí pearsanta, eadhon:

a) **Fógra** i ndáil le sárú sonraí **don DPC**, mura bhfuil ar chumas an rialaitheora a léiriú nach dóigh go mbeidh riosca ann do na hábhair sonraí mar thoradh ar an sárú; agus

b) An sárú **a chur in iúl** do na **hábhair sonraí**, sa chás go bhféadfadh ardriosca do na hábhair sonraí a bheith mar thoradh ar an sárú**.**

Tá sé tábhachtach go mbeidh tuiscint ag rialaitheoirí, nach mór dóibh, ar an bpointe boise is a fhaigheann siad amach faoi shárú i ndáil le sonraí pearsanta, tús a chur le hamchlár. Ní mór do rialaitheoirí Airteagal 33(1) den GDPR a chomhlíonadh trí fhógra a thabhairt don DPC gan mhoill mhíchuí (tráth nach deireanaí ná 72 uair an chloig faoin GDPR). Sa bhreis air sin, sa chás gur infheidhme, ní mór do rialaitheoirí an sárú i ndáil le sonraí pearsanta a chur in iúl do na hábhair sonraí gan mhoill mhíchuí, chun Airteagal 34(1) a chomhlíonadh.

Ní mór do rialaitheoirí a chinntiú freisin, ag teacht lena gcuid oibleagáidí faoi phrionsabal na cuntasachta agus ceanglais Airteagal 33 den GDPR, go bhfuil sé ar a gcumas a léiriú, trí thaifid agus trí nósanna imeachta chuí, go bhfuil na hoibleagáidí maidir le fógra á

gcomhlíonadh acu, go háirithe amlínte ó thaobh fógra a thabhairt don DPC '*gan mhoill mhíchuí*'.

Ní mór go mbeidh rialaitheoirí ar an eolas agus iad ag tabhairt fógra don DPC i ndáil le sárú sonraí pearsanta, go bhféadfadh siad, más gá, tuilleadh faisnéise agus uasdátaithe a thabhairt don DPC tar éis dóibh an fógra tosaigh a bheith tugtha acu. Ní mór go mbeidh sé ar chumas rialaitheoirí, cúiseanna a thabhairt leis an mhoill ó thaobh na faisnéise ábhartha a chur ar fáil ón tús, de réir Airteagal 33(1).

Maidir leis seo, moltar i dTreoirlínte Mheitheal Oibre Airteagal 29[10], nuair a chuireann an rialaitheoir an sárú in iúl den chéad uair, gur chóir dó/di an t-údarás maoirseachta a chur ar an eolas nach bhfuil an fhaisnéis go léir atá riachtanach aige/aici go fóill agus go gcuirfear tuilleadh faisnéise ar fáil níos deireanaí. Ní bhaineann sé seo ón oibleagáid an méid faisnéise maidir le hábhar agus is féidir a chur ar fáil san fhógra tosaigh chuig an DPC agus níor chóir go mbeadh moill mhíchuí i gceist.

Measúnú Riosca

Ní mór don rialaitheoir, nuair atáthar ag déanamh measúnú ar shárú i ndáil le sonraí pearsanta, líon critéir a bhreithniú le linn a bheith i mbun cinneadh a dhéanamh maidir leis an riosca atá ann do chearta agus do shaoirsí na n-ábhar sonraí atá faoi thionchar, lena n-áirítear:

- nádúr agus imthosca an tsáraithe;
- an cineál sonraí pearsanta atá faoi thionchar (lena n-áirítear cibé an bhfuil sonraí pearsanta atá íogair nó an bhfuil 'catagóir speisialta' sonraí pearsanta i gceist);
- an méid sonraí pearsanta atá i gceist;
- féidearthacht na sonraí pearsanta a úsáid go mailíseach;
- an damáiste nó an díobháil féideartha a d'fhéadfadh a bheith ann do na hábhair sonraí; agus
- na céimeanna atá glactha nó an fhéidearthacht an damáiste nó an díobháil a mhaolú;

Ba chóir do rialaitheoirí béim áirithe a chur ar bhreithniú cibé an bhféadfaí sonraí pearsanta, nó an dóigh go bhféadfaí sonraí pearsanta a úsáid ar bhealach mailíseach nuair atáthar ag déanamh measúnú ar an riosca a d'fhéadfadh a bheith ann do na hábhair sonraí atá faoi thionchar. I gcásanna ina bhfuil an fhéidearthacht aitheanta ó thaobh úsáid mhailíseach a bhaint as sonraí, ní mór don rialaitheoir mionsonraí maidir

[10] Treoirlínte Mheitheal Oibre Airteagal 29 Leathanach 14-16

leis na gníomhartha sonracha maolaithe a glacadh a chur ar fáil don ábhar/do na hábhair sonraí agus an chomhairle ábhartha maidir leis an mbealach a bhféadfadh na hábhair sonraí iad féin a chosaint ó iarmhairtí dochracha an tsáraithe.

Ní mór don rialaitheoir athbhreithniú a dhéanamh ar na heachtraí sáraithe go léir a cuireadh in iúl, sa chás go bhfuil féidearthacht aitheanta ann ó thaobh úsáid mhailíseach a bhaint as sonraí agus é mar aidhm a dheimhniú cibé a raibh iarrachtaí déanta le húsáid mhíchuí a bhaint as aon sonraí pearsanta. Ní mór mionsonraí maidir le hathbhreithnithe den sórt sin a chur ar fáil don DPC mar uasdátú ar fhógraí sáraithe atá tuairiscithe.

Sa chás, tar éis breithniú cúramach agus tar éis céimeanna maolaithe cuí a ghlacadh, go dtagann rialaitheoir sonraí ar an gconclúid *'nach dóigh go mbeidh an sárú ina riosca do chearta agus do shaoirsí na n-ábhar sonraí'*, is ansin a bheidh ar chumas an rialaitheora sonraí an cinneadh a dhéanamh gan fógra i ndáil le sárú a chur faoi bhráid an DPC. Ní mór measúnuithe riosca a bhreithniú ar bhonn cás ar chás agus ní mór taifead a choinneáil mar chuid den dualgas ginearálta, sé sin cothabháil a dhéanamh ar thaifid maidir le sáruithe.

Faisnéis atá le Cur ar Fáil

Ní mór don rialaitheoir, nuair atá sé/sí ag tabhairt fógra don DPC i ndáil le sárú sonraí pearsanta, chun cuidiú leis an DPC ó thaobh athbhreithniú a dhéanamh ar an bhfógra, a bheith in ann an méid seo a leanas a chur ar fáil:

- cur síos mionsonraithe ar an mbealach ar tharla an sárú;
- taifead maidir le conas agus cén uair a fuair siad amach faoin sárú;
- cur síos mionsonraithe ar fhoinse an tsáraithe;
- cá mhéad ábhar sonraí atá faoi thionchar;
- na catagóirí sonracha sonraí atá faoi thionchar;
- céard iad na céimeanna a glacadh ar an bpointe boise is a fuarthas amach faoin sárú;
- aon phleananna/céimeanna amach anseo atá le glacadh agus an t-achar ama lena dtabhairt isteach;
- cibé an bhfuil na taifid ábhartha go léir, ar nós taifid iniúchóireachta coinnithe;
- taifead den phróiseáil; agus
- doiciméadú beartas agus nósanna imeachta ábhartha.

Sa chás gur gá tuilleadh faisnéise a chur faoi bhráid an DPC maidir le sárú, ní mór é sin a dhéanamh gan mhoill mhíchuí. Sa chás go n-eisíonn an DPC tuilleadh ceisteanna maidir

leis an eachtra sáraithe, ní mór freagraí a chur ar fáil laistigh den spriocdháta atá leagtha amach ag an DPC.

Sa chás go measann an rialaitheoir an riosca do chearta agus shaoirsí na n-ábhar sonraí a bheith 'Ard', ní mór don rialaitheoir an sárú i ndáil le sonraí pearsanta a chur in iúl do na hábhair sonraí atá faoi thionchar gan mhoill mhíchuí. Ní mór cur síos atá i dteanga atá soiléir agus simplí a bheith sa chumarsáid chuig do na hábhair sonraí atá faoi thionchar maidir le nádúr an tsáraithe i ndáil le sonraí pearsanta agus an méid seo a leanas ar a laghad a bheith ann:

- ainm agus mionsonraí teagmhála an oifigigh cosanta sonraí nó pointe teagmhála eile inar féidir tuilleadh faisnéise a fháil;
- Iarmhairtí dóchúla an tsáraithe i ndáil le sonraí pearsanta; agus
- Na bearta a glacadh nó atá beartaithe ag an rialaitheoir a ghlacadh le haghaidh a thabhairt ar an sárú i ndáil le sonraí pearsanta, lena n-áirítear, sa chás gur cuí, bearta le tionchair dhochracha a d'fhéadfadh a bheith ann a mhaolú.

Beartas agus Nós Imeachta maidir le Sárú i nDáil le Sonraí Pearsanta

Ní mór do rialaitheoirí a gcuid beartas agus nósanna imeachta féin a fhorbairt maidir le déileáil le sáruithe i ndáil le sonraí pearsanta. Agus é sin á dhéanamh acu, b'fhéidir gur mhian le rialaitheoir breithniú a dhéanamh ar nós imeachta oibríochta caighdeánach a fhorbairt agus a úsáid chun feidhmiú mar threoir do fhreagra na heagraíochta i ndáil le heachtraí sáraithe sonraí pearsanta agus le breac-chuntas a thabhairt ar an nós imeachta maidir le sárú inmheánach.

D'fhéadfadh nós imeachta oibríochta caighdeánach rialaitheora próifíl riosca do shonraí pearsana a leagan amach i ngach cuid de chóras an rialaitheora agus an fhaisnéis atá riachtanach a bheith ar láimh chun cur ar chumas an rialaitheora tabhairt faoin dá chéim den mheasúnú riosca. Cuideoidh sé sin le cad ba chóir don eagraíocht a dhéanamh roimh, le linn agus tar éis na heachtra sáraithe.