Treoirlínte d'Eagraíochtaí atá ag Fostú Soláthróirí Néalseirbhísí

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Clár an Ábhair

Ar cheann de na príomhoibleagáidí faoin Rialachán Ginearálta maidir le Cosaint Sonraí (GDPR) d'eagraíochtaí a dhéanann próiseáil ar shonraí pearsanta ('rialaitheoirí'), nach mór dóibh é sin a dhéanamh ar bhealach a chinntíonn slándáil chuí sonraí pearsanta, lena n-áirítear, cosaint in aghaidh próiseáil neamhúdaraithe agus neamhdhleathach (lena n-áirítear, goid, scrios nó damáiste nó nochtadh) agus úsáid á bhaint as 'bearta teicniúla nó eagraíochtúla cuí'. Tagraítear dó seo uaireanta mar phrionsabal 'sláine agus rúndachta' nó 'prionsabal slándála'.

Is oibleagáid thábhachtach atá san oibleagáid seo, agus ceann nach mór do rialaitheoirí a bheith ar an eolas fúithi, go háirithe iad siúd a bhaineann úsáid as nó a stórálann sonraí pearsanta atá íogair. Tá, cibé an bhfuil nó nach bhfuil bearta iomchuí teicniúla agus eagraíochtúla i bhfeidhm ag eagraíocht le slándáil na sonraí pearsanta atá á bpróiseáil acu a chinntiú, ar cheann de na chéad cheisteanna is dóigh a bheidh á cur ag an gCoimisiún um Chosaint Sonraí (DPC) i gcás sárú i ndáil le sonraí pearsanta nó ó thaobh feidhmiú cumhachtaí imscrúdaithe an DPC. Is féidir le rialaitheoirí comhairle a lorg freisin sa treoir do rialaitheoirí maidir le slándáil sonraí le linn dóibh a bheith i mbun measúnaithe ar na bearta iomchuí slándála nach mór dóibh a chur i bhfeidhm.

Tá líon atá ag dul i méid de sheirbhísí ann a bhfuil 'néalstóráil' á tairiscint acu, a chuireann an deis ar fáil le doiciméid, grianghraif, físeáin agus comhaid eile a uaslódáil agus a stóráil ar chianfhreastalaí, le comhroinnt cianrochtana a chumasú nó chun feidhmiú mar chóip chúltaca. Tá úsáid aon chineál néalseirbhísí mar chuid dá ngnó mar réimse tábhachtach nach mór d'eagraíochtaí a chinntiú go bhfuil slándáil leordhóthanach ann ó thaobh na sonraí pearsanta atá á bpróiseáil acu.

D'fhéadfadh riosca do shlándáil sonraí pearsanta a theacht chun cinn nuair a thugann rialaitheoir sonraí smacht ar na sonraí ar láimh do sholáthróir néalseirbhíse, sá chás nach bhfuil faisnéis leordhóthanach ar fáil maidir le próiseáil na néalseirbhísí agus leis na cosaintí atá i bhfeidhm nó sa chás nach bhfuil ar chumas an tsoláthróra néalseirbhíse tacaíocht leordhóthanach a thabhairt d'oibleagáidí an rialaitheora sonraí nó do chearta an ábhair sonraí.

Ní mór do rialaitheoir sonraí smacht a bheith aige/aici i gcónaí ar na sonraí pearsanta a bhailíonn sé/sí nuair a ligean sé/sí próiseáil na sonraí sin ar fhochonradh le soláthróir néalseirbhíse. Baineann príomhghné den smacht le **slándáil** na sonraí a chinntiú. Ní mór do rialaitheoirí (cliaint agus soláthróirí néalseirbhísí araon) a bheith **trédhearcach** freisin maidir le próiseáil sonraí pearsanta. Tá **suíomh** na sonraí tábhachtach do smacht agus do shlándáil. Ar shaincheist ghaolmhar freisin tá an riachtanas maidir le **conradh i scríbhinn**.

Cad is 'néalríomhaireacht ann?

Ciallaíonn daoine rudaí difriúla agus iad ag caint faoi phróiseáil sonraí 'sa néalríomhaireacht'. Ciallaíonn sé, de ghnáth, eagraíocht atá ag próiseáil sonraí pearsanta a bhaineann úsáid as soláthróir néalseirbhíse seachtrach chun cuid den phróiseáil nó an phróiseáil go léir a dhéanamh nó na seirbhísí a stóráil ar fhreastalaithe atá faoi smacht an tsoláthróra. In go leor cásanna, beidh na soláthróirí néalseirbhíse seachtracha ag feidhmiú mar 'phróiseálaithe' sonraí, lena bhfuil líon freagrachtaí ag gabháil leis faoin GDPR, cé nach mbeidh na freagrachtaí ar leibhéal chomh hard céanna is atá na freagrachtaí atá ar rialaitheoirí. Is ionann próiseálaí agus duine nó eagraíocht ar bith a phróiseálann sonraí thar ceann nó ar threoracha rialaitheora.

Go ginearálta, tá trí shamhail seirbhíse difriúla néalríomhaireachta ar fáil d'eagraíochtaí. San fhoirm is sofaisticiúla, tugann an soláthróir néalríomhaireachta aire do gach gné de na sonraí thar ceann an chliaint, seachas na sonraí loma a chuireann úsáideoirí aonair isteach. Mar sin, cuireann an eagraíocht néalríomhaireachta an méid seo a leanas ar fáil:

- ☑ an bonneagar fisiciúil i lárionad sonraí;
- ☑ an córas oibríochta leis na bogearraí riachtanacha a rith; agus
- ☑ na bogearraí atá riachtanach leis na sonraí féin a phróiseáil.

Tagraítear dó seo uaireanta mar 'Bogearraí mar Sheirbhís' nó 'SaaS'.

D'fhéadfadh cliant (an rialaitheoir sonraí) gan ach cuid amháin den tseirbhís atá ar fáil ón soláthróir néalseirbhíse a roghnú freisin – mar shampla, spás freastalaí amháin (a dtagraítear dó uaireanta mar 'Bonneagar mar Sheirbhís' nó 'IaaS') nó spás freastalaí chomh maith le huirlisí bogearraí (a dtagraítear dó uaireanta mar 'Ardán mar Sheirbhís' nó 'PaaS').

Ar dhifríocht eile a dhéantar go minic idir 'néal príobháideach – nuair a dhíríonn soláthróir acmhainní ar chliant sonrach - 'néal poiblí' – áit inar féidir leis an gcliant

feidhmiú i dtimpeallacht ilúsáideora lena mbaineann córais agus bonneagair comhroinnte. D'fhéadfadh leaganacha 'hibride' den mhéid atá thuas a bheith ann, áit a bhfuil meascán de phróiseáil agus de chomhroinnt sonraí idir bhonneagar an rialaitheora féin agus bonneagar an tsoláthróra neálseirbhíse.

Go ginearálta cuireann soláthróirí néalseirbhíse seirbhísí próiseála ar fáil do rialaitheoirí sonraí ach d'fhéadfadh siad seirbhísí fophróiseála a chur ar fáil do sholáthróirí eile. I roinnt cásanna, áfach, tá soláthróirí néalseirbhíse ina rialaitheoirí sonraí freisin nó ina 'gcomhrialaitheoirí'. I gcásanna den sórt sin, tá siad faoi réir ag oibleagáidí atá níos troime faoin GDPR seachas mar a bhíonn siad agus iad ag feidhmiú mar phróiseálaí. Tugtar aghaidh go príomha sa treoir seo ar sholáthróirí néalseirbhíse atá ag feidhmiú mar phróiseálaithe agus na rialaitheoirí a bhíonn rannpháirteach leo.

Cad iad na breithnithe slándála thart ar néalríomhaireacht?

Éilíonn Airteagal 28(1) de GDPR nár chóir do rialaitheoir ach próiseálaithe a bhfuil sé ar a gcumas ráthaíochtaí leordhóthanacha chun bearta teicniúla agus eagraíochtúla cuí a chur i bhfeidhm, a fhostú. Chomh maith leis sin, ceanglaítear faoi Airteagal 32 den GDPR go gcuireann an rialaitheoir agus an próiseálaí bearta teicniúla agus eagraíochtúla cuí i bhfeidhm leis an leibhéal slándála cuí i leith riosca a chinntiú. Féadfar úsáid a bhaint as cód iompair ceadaithe (Airteagal 40 den GDPR) nó meicníocht deimhniúcháin ceadaithe chun cur le comhlíonadh Airteagal 32 den GDPR. Dá bhrí sin, ní mór do rialaitheoir a bheith sásta go mbeidh sonraí pearsanta slán má dhéantar iad a chur amach ar chonradh chuig soláthróir néalseirbhíse.

Tá dhá phríomhghné ag gabháil le slándáil sa chomhthéacs seo:

- Ar an gcéad dul síos, ní mór don rialaitheoir a bheith sásta go ndéanfaidh an próiseálaí (an soláthróir néalseirbhíse) na sonraí a phróiseáil de réir treoracha an rialaitheora agus sin amháin. Tá baint dhíreach aige seo leis an ngá atá le conradh a bheith idir an rialaitheoir agus an soláthróir néalseirbhíse.
- Ar an dara dul síos, ní mór don rialaitheoir a bheith sásta go bhfuil na rioscaí atá ann ó scriosadh neamhdhleathach nó trí thionóisc, cailleadh, athrú nó nochtadh neamhúdaraithe, nó rochtain chuig sonraí pearsanta atá a dtarchur, á stóráil nó á bpróiseáil ar shlí eile, tógtha san áireamh ag an soláthróir néalseirbhíse.

Ní mór do rialaitheoir a bheith sásta, sula mbreithníonn sé/sí sonraí pearsanta a chur faoi chúram soláthróra néalseirbhíse, go bhfuil caighdeáin slándála an tsoláthróra néalseirbhíse leordhóthanach agus cuí do phróiseáil na sonraí pearsanta a dtabharfaidh siad fúthu thar ceann an rialaitheora. Ní mór go mbeidh ar chumas an tsoláthróra néalseirbhíse gealltanais a thabhairt ar phríomhshaincheisteanna ar nós:

☑ Bréagainmniú agus criptiú sonraí pearsanta más gá.

☑ Leithlisiú nó deighilt sonraí pearsanta a chuireann an rialaitheoir ar fáil ó shonraí custaiméirí eile an tsoláthróra néalseirbhíse.

- ☑ An cumas rúndachta, ionracas, fáil agus teacht aniar na gcóras agus na seirbhísí próiseála a chinntiú. Cuimsítear anseo bealaí eagraíochtúla agus teicniúla, ó riachtanais rúndachta foirne chomh fada le freastal ar cheanglais slándála Airteagal 32 den GDPR.
- ☑ An cumas fáil agus rochtain sonraí pearsanta a thabhairt ar ais ar bhealach tráthúil i gcás eachtra fisiciúil nó teicniúil.
- ☑ Próiseas le tástáil, measúnú agus meastóireacht rialta a dhéanamh ar éifeachtúlacht bearta teicniúla agus eagraíochtúla chun slándáil na próiseála a chinntiú.
- ☑ Nósanna imeachta i gcás sárú i ndáil leis na sonraí. Ciallóidh sé seo go praiticiúil, plean freagartha ó thaobh eachtra a bheith i bhfeidhm agus go ndéantar comhaontú ceangailteach idir an próiseálaí agus an rialaitheoir ionas nach gcuirfear ábhair sonraí i mbaol agus gan ghá leis.
- ☑ Bealaí leis na sonraí pearsanta go léir a scriosadh nó a thabhairt ar ais don rialaitheoir nuair a thagann an conradh chun críche.

Ní mór do chliant na néalseirbhíse a bheith lánchinnte maidir leis na hábhair thuas, ar mhaithe leo féin, sula bhfostaíonn siad soláthróir néalseirbhíse áirithe agus ar fud aon socrú conartha a dtagann siad air leis an soláthróir néalseirbhíse. De ghnáth, cuirfear an méid sin i gcrích trí anailís theicniúil mionsonraithe a chuimseoidh ceistneoir slándála faisnéise chuig an soláthróir néalseirbhíse agus/nó cód iompair nó meicníocht dheimhniúchán a chuirfeadh an soláthróir néalseirbhíse ar fáil mar dhearbhú. I roinnt cásanna, d'fhéadfadh sé go mbeadh sé riachtanach cigireacht a dhéanamh ar an áitreabh freisin, ar an mbealach a bhfuil a mbeartas slándála curtha i bhfeidhm ag an eagraíocht nó iniúchadh a dhéanamh ar oibríochtaí próiseála sonraí pearsanta áirithe nó ar úsáid teicneolaíochta.

Cad iad na riachtanais trédhearcachta?

Ionas go mbeidh tuiscint ag rialaitheoir ar an mbealach ina mbeidh soláthróir néalseirbhíse in ann freastal ar a gcuid riachtanais próiseála ar bhealach a chomhlíonann an GDPR, tá leibhéal ard trédhearcachta riachtanach. Ciallaíonn sé seo nach mór don soláthróir néalseirbhíse míniú a thabhairt maidir lena gcuid oibríochtaí próiseála chun sástacht na gcustaiméirí. Ní mór go mbeidh ar chumas rialaitheoirí faisnéis thrédhearcach a chur ar fáil freisin do na hábhair sonraí go bhfuiltear chun seirbhísí néalphróiseála a úsáid chun próiseáil a dhéanamh ar a gcuid sonraí pearsanta. Dá bhrí sin, is gné thábhachtach atá i dtrédhearcacht ó thaobh na cinnteoireachta a bhíonn a dhéanamh ag daoine aonair agus iad ar tí leas a bhaint as seirbhísí rialaitheora.

Mar atá tugtha ar aird thuas, d'fhéadfadh sé go mbeadh ceistneoir iniúchta leordhóthanach i roinnt cásanna chun freastal ar oibleagáidí an tsoláthróra néalseirbhíse faoi Airteagal 28(3)(h) den GDPR, a thugann an deis do rialaitheoir iniúchtaí a dhéanamh ar a gcuid oibríochtaí. Díreoidh páirt lárnach den iniúchadh seo ar shocruithe slándála. Tabhair ar aird, go bhféadfadh sé, go mbeidh seirbhísí á gcur ar

fáil, de ghnáth, ag soláthróirí néalseirbhíse do go leor rialaitheoirí sonraí ag an am céanna agus go bhfuil siad faoi réir ag oibleagáidí slándála agus rúndachta i ndáil le gach aon rialaitheoir, agus go mbeidh méid agus mionsonraí an ábhair a bheidh á chur ar fáil acu san iniúchadh teoranta.

Tá feidhm freisin le hAirteagal 30(2) den GDPR ar choinneáil taifead i gcás soláthróirí néalseirbhíse. Ciallaíonn sé seo, mar chuid de cheanglais chuntasachta an GDPR, gur chóir do phróiseálaí doiciméadú a dhéanamh agus a bheith in ann an fhaisnéis bhunúsach a sonraítear a chur ar fáil don rialaitheoir.

Ní mór do sholáthróirí néalseirbhíse, faoi Airteagal 28(2) agus 28(4) den GDPR, mar phróiseálaithe, faisnéis maidir le haon fo-phróiseálaithe atá á fhostú acu chun a gcuid seirbhísí a sholáthar a chur ar fáil dá gcuid rialaitheoirí. Ciallaíonn sé seo gur féidir le rialaitheoir athbhreithniú a dhéanamh ar an socrú seo faoi théarmaí an chonartha agus tugann sé an deis don rialaitheoir cur i gcoinne fo-phróiseáil más gá.

Leagtar amach in Airteagal 28(5) den GDPR gur féidir le soláthróir néalseirbhíse, mar phróiseálaí, leas a bhaint as cóid iompair ceadaithe nó meicníochtaí deimhniúcháin ceadaithe chun cuidiú le comhlíonadh a léiriú i leith gnéithe dá bpróiseáil. Tá sé tábhachtach, go mbíonn nádúr, scóip agus comhthéacs cóid nó deimhniúcháin den sórt sin soiléir do rialaitheoir ionas go mbeidh tuiscint leordhóthanach acu ar an méid a bhaineann sé le próiseáil a gcuid sonraí pearsanta agus má tá sé cuí ó thaobh na n-oibríochtaí próiseála atá á gcur faoi chonradh.

An cuma cá bhfuil na sonraí lonnaithe?

Baineann sonraí pearsanta atá á gcoinneáil laistigh den Limistéar Eorpach Eacnamaíoch (EEA) (Ballstáit an AE chomh maith leis an Íoslainn, Lichtinstéin agus an Iorua) buntáistí as comhchaighdeán cosanta a leagtar síos ag leibhéal AE. Ní mór, nuair a aistrítear sonraí chuig tíortha lasmuigh den EEA, bearta speisialta a ghlacadh lena chinntiú go bhfuil cosaint leordhóthanach á fháil ag na sonraí i gcónaí. Leagtar amach an raon roghanna i dtreoir an DPC ar aistrithe idirnáisiúnta. Go praiticiúil, sa chás go mbíonn soláthróir néalseirbhíse ag próiseáil sonraí pearsanta lasmuigh den EEA, ní mór a bheith ag brath ar cheann de na meicníochtaí seo a leanas:

- ☐ Go ndéantar na sonraí a aistriú bunaithe ar chinneadh leordhóthanachta,[1] mar a shonraítear in Airteagal 45 den GDPR
- ☐ Tá aistriú na sonraí faoi réir ag cosaintí cuí (ar nós conarthaí ar leagan ceadaithe an AE) mar a shonraítear in Airteagal 46 den GDPR

[1] Féach Cinntí Leordhóthanacha an Choimisiúin Eorpaigh, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

- ☐ Tá aistriú na sonraí faoi réir ag rialacha corparáideacha ceangailteacha de réir Airteagal 47 den GDPR

Sa chás go mbaintear úsáid as 'leagan conarthaí' nó 'rialacha corparáideacha ceangailteacha' tá sé tábhachtach go gclúdaíonn na cosaintí atá á gcur ar fáil ag na meicníochtaí seo aon fho-conraitheoirí atá fostaithe ag an soláthróir néalseirbhíse.

Cén saghas conartha a theastaíonn chun néalseirbhís a úsáid?

Éilíonn Airteagal 28(3) den GDPR go mbíonn an phróiseáil a bhíonn á déanamh ag próiseálaí faoi rialú ag conradh. Chomh maith leis sin, mar atá tugtha ar aird thuas, níor chóir do phróiseálaí aon phróiseálaí eile a fhostú gan údarú ón rialaitheoir. Ciallaíonn sé sin, go gcoinníonn rialaitheoir atá ag fostú soláthróir néalseirbhíse mar phróiseálaí smacht ar na sonraí pearsanta atá á bpróiseáil acu, go bhfuil teorainneacha comhaontaithe agus soiléire leis an bpróiseáil seo, go bhfuil an próiseálaí soiléir maidir lena gcuid oibleagáidí don rialaitheoir agus go sainmhínítear aon teorainneacha i leith freagrachta agus dliteanas as sárú ó thaobh an phróiseálaí (soláthróir néalseirbhíse).

Ní mór go n-áireoidh conarthaí na príomhphointí a bhfuil breac-chuntas tugtha ina leith thíos:

- ☑ Nach ndéanfaidh an soláthróir néalseirbhíse – agus aon fho-phróiseálaithe atá á n-úsáid ag an soláthróir – próiseáil ar shonraí ach de réir treoir an rialaitheora sonraí.
- ☑ Dearbhú mionsonraithe an tsoláthróra néalseirbhíse ar bhearta slándála agus maidir leis an mbealach a fhreastalófar ar cheanglais faoi Airteagal 32 den GDPR.
- ☑ Liosta de na fo-phróiseálaithe atá á bhfostú ag an bpróiseálaí agus mionsonraí maidir leis an mbealach a chaithfear leis na nuashonrúcháin seo don rialaitheoir.
- ☑ An fhaisnéis atá riachtanach le comhlíontacht an tsoláthróra néalseirbhíse le hAirteagal 28 den GDPR a léiriú agus an bealach ina gceadóidh nó a gcuideoidh an próiseálaí le hiniúchtaí nó cigireacht an rialaitheora.
- ☑ Na bearta atá á soláthar chun slándáil sonraí pearsanta atá á bpróiseáil lasmuigh den Limistéar Eorpach Eacnamaíoch a dhearbhú.
- ☑ An dliteanas atá á leithroinnt idir an rialaitheoir agus an próiseálaí i gcás sárú GDPR nó sárú i ndáil le sonraí pearsanta agus maidir le conas a chuirfear cásanna den sórt sin in iúl don rialaitheoir
- ☑ An bealach ina bhfuil an próiseálaí ag freastal ar a chuid/ar a cuid oibleagáidí ó thaobh tacú le cearta na n-ábhair sonraí.
- ☑ Dlínse ábhair, scóip, comhthéacs, cuspóir agus achar na próiseála agus conas a dhéileálfar leis na cineálacha agus na catagóirí sonraí pearsanta ag tús, aistriú, gnáthphróiseáil agus 'deireadh ré' – lena n-áirítear, tabhairt ar ais nó scriosadh.

Tá tuilleadh faisnéise ar fáil maidir le conradh den sórt sin a chur le chéile i dtreoir phraiticiúil ar chonarthaí próiseálaí sonraí an DPC, ar láithreán gréasáin an DPC.

Tuilleadh Treorach

Tá treoir úsáideach curtha ar fáil ag an nGníomhaireacht Eorpach um Shlándáil Gréasáin agus Faisnéise (ENISA), atá scríofa ó thaobh dearcadh na hEorpa ar ábhair, lena n-áirítear, 'I dtreo coinbhéirseacht shlán Néal agus IoT', 'Treoirlínte Teicniúla d'fheidhmiú íosbhearta slándála do Sholáthróirí Seirbhís Dhigiteach', agus 'Treoir Shlándála Néal do SME'nna'.

Tá Treoirlínte ar úsáid seirbhísí néalríomhaireachta ag institiúidí agus ag comhlachtaí Eorpacha foilsithe ag an Maoirseoir Eorpach um Chosaint Sonraí (EDPS), atá freagrach as cosaint sonraí in institiúidí AE, a d'fhéadfadh a bheith úsáideach (cé go bhfuil siad bunaithe ar shraith dlíthe atá beagán difriúil) d'eagraíochtaí atá ag iarradh tuilleadh tuisceana a fháil ar shlándáil néal.

Meabhraítear d'eagraíochtaí nach mór, sáruithe sonraí pearsanta faoin GDPR a thuairisciú don údarás maoirseachta ábhartha sa chás go mbíonn an sárú ina chúis le riosca do na daoine aonair atá faoi thionchar. Ní mór d'eagraíochtaí tabhairt faoi sin laistigh de 72 uair an chloig ó fhaigheann siad amach faoin sárú. Sa chás gur dóigh go mbeidh ardriosca do na daoine aonair atá faoi thionchar mar thoradh ar an sárú, ní mór d'eagraíochtaí na daoine aonair sin a chur ar an eolas gan mhoill míchuí. Tá tuilleadh treoracha ar fhógraí i ndáil le sáruithe le fáil ar láithreán gréasáin an DPC.