| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe | | | | | | |
| Uimhir an doiciméid:<br>P17 | | | | | Teideal an doiciméid:<br>**Beartas um Chosaint Sonraí agus Príobháideachas** | | | | | | |
| Leagan:<br>1.0 | | Dáta teacht i bhfeidhm:<br>01.01.2025 | | | Úinéir an doiciméid: | | | | | | |
| X | Beartas | | Caighdeán | | Nós imeachta | | Foirm | | Clár | | Eile |

| **Stair na n-athbhreithnithe** | | | | |
|---|---|---|---|---|
| **Uimhir na hathbhreithnithe** | **Dáta na hathbhreithnithe** | **Athruithe** | **Athbhreithnitheag** | **Úinéir an phróisis** |
| | | | | |
| | | | | |

| **Formheasanna** | | | |
|---|---|---|---|
| **Ainm** | **Post** | **Dáta** | **Síniú** |
| | | | |
| | | | |

Ailíniú le caighdeáin agus rialacháin

| Caighdeán/Rialachán | Clásal/Airteagal | Nóta |
|---|---|---|
| ISO/IEC 27001:2022 | Clásail 5.1, 6.1.3, 8.1, 10 | Rialuithe ginearálta, teicniúla agus feabhsúcháin leanúnaigh a bhaineann le cosaint sonraí |
| ISO/IEC 27002:2022 | Rialuithe 5.34, 8.10, 8.11, 8.12 | Rialuithe maidir le láimhseáil PII, coinneáil, scriosadh, anaithnidiú agus cearta ábhar sonraí |
| NIST SP 800-53 Rev.5 | AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23 | Ceanglais maidir le rialachas, riosca, bainistiú rochtana, logáil, freagairt do sháruithe agus clár príobháideachais |
| GDPR an Aontais Eorpaigh | Airteagail 5, 6, 12–23, 25, 28, 30, 32–34; Aithris 78 | Gach croícheanglas príobháideachais, cuntasachta, cearta ábhar sonraí, iarrataí ó ábhair sonraí, sáruithe agus prionsabail an deartha agus an réamhshocraithe |
| NIS2 an Aontais Eorpaigh | Airteagal 21(2)(e), (f) | Rialuithe slándála bunaithe ar riosca d'eintitis riachtanacha agus thábhachtacha |
| DORA an Aontais Eorpaigh | Airteagail 6(2)(d), 11(1)(c), 15(1), 17 | Rialachas, riosca tríú páirtí agus amlínte slána próiseála |
| COBIT 2019 | APO12, DSS01, DSS05, MEA | Bainistiú riosca, oibríochtaí slána, faireachán ar chomhlíonadh |

**1. Cuspóir**

1.1 Leagtar síos sa bheartas seo prionsabail eagraíochtúla éigeantacha agus ceanglais theicniúla maidir le cosaint sonraí pearsanta agus le cur chun feidhme príobháideachais trí dhearadh i ngach timpeallacht.

1.2 Sainítear leis freagrachtaí na heagraíochta faoi chaighdeáin idirnáisiúnta agus faoi chreataí rialála chun a chinntiú go mbailítear, go bpróiseáiltear, go gcoinnítear, go roinntear agus go ndiúscraítear sonraí pearsanta go dleathach, go slán agus go trédhearcach.

1.3 Treisíonn an beartas seo freisin comhlíonadh na ndlíthe agus na gcreataí príobháideachais is infheidhme, lena n-áirítear Rialachán Ginearálta an Aontais Eorpaigh maidir le Cosaint Sonraí (GDPR), Treoir NIS2 an Aontais Eorpaigh, an tAcht um Athléimneacht Oibríochtúil Dhigiteach (DORA) de chuid an Aontais Eorpaigh, ISO/IEC 27001:2022 agus COBIT 2019.

**2. Raon feidhme**

**2.1 Baineann an beartas seo le gach aonad eagraíochtúil, ball foirne agus córas atá páirteach i bpróiseáil sonraí pearsanta, lena n-áirítear:**

2.1.1 Fostaithe, conraitheoirí, sainchomhairleoirí agus soláthraithe seirbhíse tríú páirtí.

2.1.2 Sonraí a bhailítear ó fhoinsí inmheánacha agus seachtracha ar fud gach feidhme gnó.

2.1.3 Meáin fhisiciúla agus dhigiteacha, lena n-áirítear seirbhísí néalríomhaireachta, ardáin SaaS, gléasanna soghluaiste agus taifid pháipéarbhunaithe.

2.1.4 Gach timpeallacht, lena n-áirítear córais táirgthe, forbartha, tástála agus cúltaca ina bhféadfadh sonraí pearsanta a bheith ann.

**2.2 Cumhdaíonn sé gach gníomhaíocht phróiseála a rialaítear faoi na dlíthe agus na caighdeáin phríobháideachais is infheidhme, lena n-áirítear, ach gan a bheith teoranta do:**

2.2.1 Bailiú, stóráil, úsáid, tarchur agus diúscairt sonraí pearsanta.

2.2.2 Cur chun feidhme chearta ábhar sonraí, doiciméadú an bhoinn dhlíthiúil agus bainistiú toilithe.

2.2.3 Aistrithe trasteorann, fógairt sáruithe agus comhroinnt sonraí le tríú páirtithe.

2.2.4 Dearadh slán agus cur chun feidhme príobháideachais de réir réamhshocraithe i gcórais agus i bpróisis.

**3. Cuspóirí**

3.1 Próiseáil dhleathach, thrédhearcach agus chuntasach sonraí pearsanta a chinntiú i gcomhréir le ISO/IEC 27001:2022 agus leis na sainorduithe dlíthiúla gaolmhara.

3.2 Prionsabail an phríobháideachais trí dhearadh agus an phríobháideachais de réir réamhshocraithe a leabú i ngach córas faisnéise, seirbhís agus próiseas gnó.

3.3 Bearta teicniúla agus eagraíochtúla (TOManna) a chur chun feidhme chun rúndacht, sláine agus infhaighteacht sonraí pearsanta a chosaint ar feadh a saolré.

3.4 Róil rialachais agus struchtúir chuntasachta um chosaint sonraí a shainiú, lena n-áirítear freagrachtaí an Oifigigh Cosanta Sonraí, na Feidhme Slándála Faisnéise, na Feidhme Dlí agus Úinéirí Sonraí.

3.5 Comhlíonadh iomlán a chumasú le hAirteagail 5, 6, 25, 30 agus 32 den GDPR, chomh maith leis na ceanglais maidir le maolú riosca agus athléimneacht faoi NIS2 agus DORA.

3.6 Cearta ábhar sonraí a chosaint, lena n-áirítear rochtain, ceartú, léirscriosadh, srianadh, iniomparthacht, agóid agus cosaint ar chinnteoireacht uathoibrithe.

3.7 Rioscaí rialála, clú, dlíthiúla agus oibríochtúla a eascraíonn as rochtain neamhúdaraithe, mí-úsáid nó caillteanas sonraí pearsanta a mhaolú.

**4. Róil agus freagrachtaí**

**4.1 An Bhainistíocht Feidhmiúcháin**

4.1.1 Soláthraíonn sí maoirseacht straitéiseach agus leithdháileann sí acmhainní leordhóthanacha chun tacú leis an gclár príobháideachais.

4.1.2 Formheasann sí an beartas seo agus cinntíonn sí go gcuirtear chun feidhme é ar fud na heagraíochta.

**4.2 An tOifigeach Cosanta Sonraí**

4.2.1 Gníomhaíonn sé/sí go neamhspleách chun maoirseacht a dhéanamh ar chomhlíonadh rialachán cosanta sonraí.

4.2.2 Coinníonn sé/sí an Taifead ar Ghníomhaíochtaí Próiseála (RoPA) de réir Airteagal 30 den GDPR.

4.2.3 Treoraíonn sé/sí rannpháirtíocht rialála, déanann sé/sí Measúnuithe Tionchair ar Chosaint Sonraí (DPIAnna) agus bainistíonn sé/sí próisis fógra sáraithe.

4.2.4 Déanann sé/sí athbhreithniú ar eisceachtaí príobháideachais agus coinníonn sé/sí an Clár Eisceachtaí Príobháideachais.

[ ... Níl ailt 4.3–8 san áireamh sa réamhamharc seo. Ceannaigh an doiciméad iomlán chun rochtain a fháil ar an gcomhábhar iomlán. ... ]

**9. Ceanglais athbhreithnithe agus nuashonraithe**

**9.1 Déanfar athbhreithniú ar an mbeartas seo ar a laghad gach bliain, nó níos luaithe faoi na coinníollacha seo a leanas:**

9.1.1 Nuashonruithe suntasacha dlíthiúla nó rialála (e.g. leasuithe ar an GDPR, spriocdhátaí DORA)

9.1.2 Córais nua nó gníomhaíochtaí próiseála nua a bhaineann le sonraí pearsanta

9.1.3 Torthaí iniúchta inmheánaigh a léiríonn bearnaí sa bheartas

9.1.4 Teagmhais sháraithe ábhartha nó aiseolas ó údarás maoirseachta

**9.2 Freagrachtaí athbhreithnithe**

9.2.1 Cuirfidh an tOifigeach Cosanta Sonraí tús le hathbhreithniú an bheartais, i gcomhordú leis an bhFeidhm Dlí, an Fheidhm Riosca, an Fheidhm Slándála Faisnéise agus an Bhainistíocht Feidhmiúcháin.

9.2.2 Ní mór gach nuashonrú a thaifeadadh i gClár Rialaithe Doiciméad an ISMS agus a dháileadh ar na páirtithe leasmhara ábhartha.

**9.3 Rialú athruithe**

9.3.1 Ní mór aon leasú ar an mbeartas seo a fhormheas go foirmiúil ag an mBainistíocht Feidhmiúcháin.

9.3.2 Déanfar leaganacha atá as feidhm a chartlannú go slán, agus ní mór stair athruithe dhoiciméadaithe a bheith sa leagan nuashonraithe.

**10. Beartais ghaolmhara agus naisc eatarthu**

10.1 P1 – Beartas Slándála Faisnéise. Leagtar amach ann na prionsabail fhoriomlána rialachais slándála atá mar bhonn leis an mbeartas príobháideachais seo. Tacaíonn P1 le rúndacht, sláine agus infhaighteacht sonraí pearsanta ar fud gach córais agus seirbhíse.

10.2 P6 – Beartas Bainistíochta Riosca. Sainmhínítear ann modheolaíocht chóireála riosca na heagraíochta, atá riachtanach chun rioscaí príobháideachais, próisis DPIA agus measúnuithe ar riosca iarmharach a mheas de réir Chlásal 6.1.3 de ISO/IEC 27001.

10.3 P13 – Beartas Aicmithe agus Lipéadaithe Sonraí. Treoraítear ann catagóiriú sonraí pearsanta agus íogaire, rud a chruthaíonn an bonn chun rialuithe príobháideachais iomchuí a chur i bhfeidhm, lena n-áirítear coinneáil, teorannú rochtana agus diúscairt shlán.

10.4 P14 – Beartas um Choinneáil agus Diúscairt Sonraí. Tacaíonn sé go díreach le ceanglais phríobháideachais faoi Airteagail 5(1)(e) agus 17 den GDPR, lena chinntiú nach gcoinnítear sonraí pearsanta ach chomh fada agus is gá agus go ndiúscraítear go slán iad de réir oibleagáidí dlíthiúla.

10.5 P16 – Beartas um Mhascadh Sonraí agus Ainm Bréige. Bunaítear ann rialuithe chun inaitheantacht sonraí pearsanta a laghdú trí bhearta teicniúla amhail tokenization, mascadh dinimiciúil agus ainm bréige, agus ar an gcaoi sin cuirtear Airteagal 32 den GDPR agus Rialú 5.34 de ISO/IEC 27002 chun feidhme.

10.6 P30 – Beartas Freagartha do Theagmhais. Leagtar amach ann na prótacail éigeantacha freagartha ar shárú a chomhtháthaíonn le láimhseáil sáruithe príobháideachais agus leis na hamlínte fógra atá riachtanach faoi Airteagail 33 agus 34 den GDPR.

10.7 P33 – Beartas Faireacháin Iniúchta agus Comhlíonta. Cuirtear ann measúnuithe sceidealaithe ar éifeachtacht an chláir phríobháideachais, ar chur chun feidhme an bheartais agus ar rianú gníomhartha ceartaitheacha ar fud aonaid eagraíochtúla agus próiseálaithe tríú páirtí.

**11. Caighdeáin agus creataí tagartha**

**11.1 ISO/IEC 27001**

11.1.1 Clásal 5.1 – Ceannaireacht agus Tiomantas: Bunaítear freagracht ar leibhéal feidhmiúcháin as cosaint sonraí pearsanta agus as cur chun feidhme phrionsabail phríobháideachais.

11.1.2 Clásal 6.1.3 – Cóireáil Riosca Slándála Faisnéise: Tacaíonn sé le sainaithint, measúnú agus cóireáil riosca príobháideachais trí DPIAnna agus eisceachtaí.

11.1.3 Clásal 8.1 – Pleanáil agus Rialú Oibríochtúil: Ceanglaítear leis coimircí teicniúla agus nós imeachta chun a chinntiú go bpróiseáiltear sonraí pearsanta go slán.

11.1.4 Clásal 10.1 – Feabhsú Leanúnach: Sainordaítear leis meastóireacht thréimhsiúil agus oiriúnú an chláir phríobháideachais.

11.2 ISO/IEC 27002:2022 Rialuithe 5.34, 8.10, 8.11, 8.12: Soláthraítear ann treoir maidir le láimhseáil PII, cur chun feidhme coinneála, scriosta, anaithnidithe agus trédhearcachta i ndáil le cearta ábhar sonraí.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AR-1, AR-2, AR-4, AR-5: Sainmhínítear rialachas, róil, cuntasacht agus freagrachtaí oiliúna príobháideachais.

11.3.2 PL-2, PL-8: Ceanglaítear leo comhtháthú rialuithe príobháideachais i saolré an chórais agus in ailtireacht na heagraíochta.

11.3.3 AC-2, AC-6: Cuirtear prionsabal na pribhléide íosta agus bainistíocht cuntas chun feidhme chun sonraí pearsanta a chosaint.

11.3.4 AU-2, AU-6, AU-9: Sainordaítear leo logáil, inrianaitheacht agus sláine iniúchta do rochtain ar shonraí pearsanta.

11.3.5 IR-4, IR-5, IR-6: Sainmhínítear próisis struchtúrtha bhrath, anailíse agus tuairiscithe do sháruithe príobháideachais.

11.3.6 PM-1, PM-21, PM-23: Bunaítear leo clár príobháideachais cuimsitheach, ailínithe le cuspóirí straitéiseacha riosca agus rialachais sonraí.

**11.4 GDPR an Aontais Eorpaigh (2016/679)**

11.4.1 Airteagail 5, 6, 12–23, 25, 28, 30, 32–34: Rialaítear leo próiseáil dhleathach, teorannú cuspóra, cearta ábhar sonraí, cuntasacht, cosaint sonraí trí dhearadh agus de réir réamhshocraithe, oibleagáidí tríú páirtí agus bainistíocht sáruithe.

11.4.2 Aithris 78: Treisítear léi prionsabail an phríobháideachais trí dhearadh.

**11.5 Treoir NIS2 an Aontais Eorpaigh (2022/2555)**

11.5.1 Airteagal 21(2)(e) agus (f): Ceanglaítear leis rialuithe slándála bunaithe ar riosca agus cosaint sonraí pearsanta a chur chun feidhme laistigh de raon feidhme eintiteas riachtanach agus tábhachtach.

**11.6 DORA an Aontais Eorpaigh (2022/2554)**

11.6.1 Airteagal 6(2)(d): Cuirtear rialachas inmheánach chun feidhme maidir le rioscaí TFC a bhaineann le láimhseáil sonraí.

11.6.2 Airteagal 11(1)(c): Sainordaítear leis maoirseacht ar riosca tríú páirtí i ndáil le seirbhísí a bhaineann le sonraí.

11.6.3 Airteagail 15(1) agus 17: Ceanglaítear leo próiseáil shlán sonraí ag soláthraithe seirbhíse agus nochtuithe maoirseachta tráthúla i ndiaidh teagmhas a bhaineann le TFC.

**11.7 COBIT 2019**

11.7.1 APO12 – Beartas Bainistíochta Riosca: Leabaítear riosca príobháideachais i maoirseacht níos leithne ar riosca fiontair.

11.7.2 DSS01 – Oibríochtaí Bainistithe agus DSS05 – Seirbhísí Slándála: Cinntítear oibríochtaí slána, lena n-áirítear rialú rochtana, coinneáil agus sláine córas.

11.7.3 MEA03 – Faireachán ar Chomhlíonadh: Ceanglaítear leis athbhreithniú leanúnach ar stádas comhlíonta i gcoinne oibleagáidí príobháideachais rialála agus beartasbhunaithe.