					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: PII14					Teideal an doiciméid: **Beartas um Shlándáil PII agus Rialú Rochtana**							
Leagan: 1.0		Dáta teacht i bhfeidhm: 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**

Ailínithe le caighdeáin agus rialacháin

Caighdeán / Rialachán	Clásal / Rialú / Airteagal	Infheidhmeacht	Cineál cumhdaigh	Nóta
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Pleanáil agus oibriú rialuithe slándála PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Fianaise, faireachán agus gníomh ceartaitheach
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Aitheantas agus cearta rochtana le haghaidh próiseáil PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Cosaint críochphointí agus fíordheimhniú slán
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logáil agus cosaint chripteagrafach
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Slándáil feidhmchlár agus ailtireacht shlán
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Cosaint agus athbhreithniú taifead
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Slándáil, cuntasacht agus rialuithe próiseálaí
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Comhtháthú rialuithe ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Treoir maidir le cur chun feidhme rialuithe slándála
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Prionsabail slándála faisnéise agus chomhlíonta príobháideachais
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4;	Both	Supporting	Rialuithe slándála um chosaint PII

	Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Raon feidhme

1.1 Sainmhíníonn an beartas seo ceanglais slándála agus rialaithe rochtana atá sonrach do PII le haghaidh córas, feidhmchlár, seirbhísí, gléasanna, timpeallachtaí scamall agus próiseas oibríochtúil a stórálann, a tharchuireann, a phróiseálann, a fhaigheann rochtain ar, a riarann nó a chosnaíonn PII.

1.2 Tá feidhm ag an mbeartas seo maidir le comhthéacsanna rialaitheora, rialaitheora chomhpháirtigh, próiseálaí agus fophhróiseálaí ina gcinnfidh, ina n-oibríonn, ina dtacaíonn nó ina mbraitheann an eagraíocht ar rialuithe slándála le haghaidh próiseáil PII.

1.3 Cumhdaíonn an beartas seo na fearainn rialaithe slándála PII seo a leanas:

1.3.1 bonnlíne slándála PII agus comhtháthú le beartais slándála faisnéise atá ann cheana;

1.3.2 rialú rochtana;

1.3.3 fíordheimhniú;

1.3.4 rochtain phribhléideach;

1.3.5 criptiú agus stóráil shlán;

1.3.6 logáil agus faireachán;

1.3.7 cumraíocht shlán agus bainistíocht leochaileachtaí;

1.3.8 rialuithe rochtana críochphointe agus scamall;

1.3.9 nascadh fianaise trí REG02, REG08, REG10 agus REG12.

1.4 Ní thagann an beartas seo in ionad Córas Bainistíochta Slándála Faisnéise iomlán, beartas slándála líonra, beartas forbartha slána, beartas cúltaca, beartas críochphointe, beartas slándála scamall, caighdeán cripteagrafach, nós imeachta bainistíochta leochaileachtaí ná nós imeachta freagartha do theagmhais. I gcás ina bhfuil na beartais sin ann cheana, sainmhíníonn an beartas seo an nasc sonrach do PII agus na ceanglais fianaise is gá le haghaidh dearbhú PIMS.

1.5 Ní dhéanann an beartas seo dúbailt ar:

1.5.1 fardal próiseála PII agus úinéireacht bonn dlíthiúil in PII03;

1.5.2 modheolaíocht riosca príobháideachais agus DPIA in PII07;

1.5.3 geataí príobháideachais de réir deartha in PII08;

1.5.4 rialacha bailithe, úsáide, nochta agus comhroinnte in PII09;

1.5.5 cur chun feidhme coinneála, scriosta agus diúscartha in PII10;

1.5.6 rialachas shaolré próiseálaí in PII12;

1.5.7 rialuithe sásra aistrithe idirnáisiúnta in PII13;

1.5.8 sreabhadh oibre teagmhais agus sáraithe in PII15;

1.5.9 rialachas faisnéise doiciméadaithe in PII17;

1.5.10 rialachas faireacháin, iniúchta agus feabhsaithe PIMS in PII18.

1.6 Chun críocha an bheartais seo, is foinsí fianaise iad logaí oibríochtúla, aschuir uirlisí slándála, easpórtálacha athbhreithnithe rochtana, tuarascálacha leochaileachta agus fianaise chumraíochta a cheanglaítear leis na réada fianaise chanónacha, a ndéantar achoimre orthu iontu, nó a dtagraítear dóibh iontu. Ní cláir PIMS ar leith iad.

2. Cuspóir

2.1 Is é cuspóir an bheartais seo a chinntiú go gcosnaítear PII le rialuithe slándála agus rochtana atá iomchuí, ailínithe le riosca agus in-iniúchta ar feadh na próiseála.

2.2 Cuireann an beartas seo ar chumas na heagraíochta a léiriú go ndéantar rialuithe slándála PII a phleanáil, a chur chun feidhme, a athbhreithniú, faireachán a dhéanamh orthu agus iad a fheabhsú

trí REG02, REG08, REG10 agus REG12 gan cláir slándála dhúblacha a chruthú ná beartais slándála faisnéise atá ann cheana a ionadú.

3. Cuspóirí

3.1 Is iad cuspóirí an bheartais seo:

3.1.1 bonnlíne rialaithe rochtana PII a shainiú le haghaidh córas agus gníomhaíochtaí próiseála;

3.1.2 a chinntiú go bhfuil rialuithe fíordheimhnithe oiriúnach do chomhthéacs íogaireachta agus rochtana PII;

3.1.3 ceanglais athbhreithnithe a shainiú maidir le rochtain phribhléideach agus gnáthrochtain ar PII;

3.1.4 ionchais maidir le criptiú agus stóráil shlán PII a shainiú i staid chiúin, faoi tharchur agus i gcomhthéacsanna ábhartha scamall nó críochphointe;

3.1.5 ionchais logála agus faireacháin a shainiú maidir le rochtain ar PII, athruithe ar PII agus riarachán PII;

3.1.6 ceanglais fianaise maidir le cumraíocht shlán agus leochaileachtaí a shainiú le haghaidh córas a phróiseálann PII;

3.1.7 ionchais rochtana críochphointe agus scamall a shainiú gan beartas iomlán críochphointe nó slándála scamall a chruthú;

3.1.8 teagmhais slándála PII amhrasta a nascadh le REG10 gan sreabhadh oibre teagmhais a dhúbailt;

3.1.9 comhtháthú le beartais slándála faisnéise atá ann cheana i gcás ina bhfuil siad ar fáil;

3.1.10 fianaise atá réidh don iniúchadh a choinneáil ag baint úsáid as REG02, REG08, REG10 agus REG12 amháin.

4. Ráitis bheartais

4.1 Bonnlíne slándála PII agus comhtháthú ISMS

4.1.1 [Both] Ní mór don Information Security Lead an bhonnlíne slándála PII a shainiú i REG12 le haghaidh gach córais nó seirbhíse a phróiseálann PII sula dtéann an córas nó an tseirbhís i dtáirgeadh nó sula ndéantar athrú ábhartha air nó uirthi.

4.1.2 [Both] Ní mór don System Owner / Application Owner suíomh na fianaise maidir leis an rialú slándála PII atá curtha chun feidhme a thaifeadadh i REG12 sula mbraithfear ar rialú slándála faisnéise atá ann cheana le haghaidh dearbhú PIMS.

4.1.3 [Controller] Ní mór don Process Owner / Business Owner íogaireacht PII, comhthéacs próiseála agus riachtanas rochtana a shainaithint i REG02 sula n-iarrfar rochtain nua nó rochtain a athraíodh go hábhartha ar PII.

4.1.4 [Processor] Ní mór don Vendor / Procurement Owner treoracha slándála custaiméara, teorainneacha freagrachta custaiméara agus gealltanais slándála an phróiseálaí a thaifeadadh i REG08 sula dtosaíonn rochtain próiseálaí ar PII custaiméara nó sula n-athraítear í go hábhartha.

4.1.5 [Both] Ní mór don Privacy Lead / PIMS Manager a fhíorú go bhfuil fianaise slándála PII nasctha le REG02, REG08, REG10 nó REG12 sula nglacfar leis an ngníomhaíocht phróiseála mar ghníomhaíocht in-iniúchta ag PIMS.

4.2 Bonnlíne rialaithe rochtana

4.2.1 [Both] Ní mór don System Owner / Application Owner rochtain ar PII a shrianadh do róil fhormheasta agus d'úsáideoirí údaraithe atá taifeadta nó inrianaithe i REG02 nó REG12 sula gcumasaítear rochtain.

4.2.2 [Both] Ní mór don Process Owner / Business Owner an cuspóir gnó le haghaidh rochtain ar PII a cheadú i REG02 nó REG12 sula soláthraíonn an System Owner / Application Owner rochtain.

4.2.3 [Both] Ní mór don System Owner / Application Owner athbhreithniú a dhéanamh ar rochtain úsáideoirí ar chórais a phróiseálann PII ardtionchair nó PII íogair ar a laghad gach ráithe agus toradh an athbhreithnithe a thaifeadadh i REG12.

4.2.4 [Both] Ní mór don System Owner / Application Owner athbhreithniú a dhéanamh ar rochtain úsáideoirí ar chórais eile a phróiseálann PII ar a laghad go bliantúil agus toradh an athbhreithnithe a thaifeadadh i REG12.

4.2.5 [Both] Ní mór don System Owner / Application Owner rochtain PII a bhaint nó a leasú i REG12 laistigh de lá gnó amháin tar éis athrú róil, foirceannadh, críochnú conartha nó nuair nach bhfuil rochtain ag teastáil a thuilleadh.

4.2.6 [Processor] Ní mór don Vendor / Procurement Owner a dhearbhú i REG08 go bhfuil rochtain próiseálaí ar PII custaiméara teoranta do threoracha custaiméara doiciméadaithe sula gcumasaítear nó sula n-athraítear rochtain.

4.2.7 [Subprocessor] Ní mór don Vendor / Procurement Owner a dhearbhú i REG08 go bhfuil rochtain fophhróiseálaí ar PII teoranta do ghníomhaíochtaí fophhróiseála údaraithe sula gcumasaítear nó sula n-athraítear rochtain fophhróiseálaí.

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

9. Eisceachtaí

9.1.1 [Both] Ní mór don Information Security Lead gach eisceacht ó cheanglas slándála nó rialaithe rochtana PII a thaifeadadh i REG12 sula ngníomhachtaítear an eisceacht.

9.1.2 [Both] Ní mór don Data Protection Officer / Privacy Advisor comhairle a thabhairt maidir le heisceachtaí slándála PII ar riosca níos airde i REG12 roimh cheadú.

9.1.3 [Both] Ní mór do Top Management eisceachtaí slándála PII a cheadú i REG12 roimh ghníomhachtú nuair a dhéanann an eisceacht difear do PII ardtionchair, PII íogair, rochtain phribhléideach, criptiú, logáil nó leochaileachtaí ardriosca gan réiteach.

9.1.4 [Both] Ní mór don Information Security Lead dáta éaga, rialú cúiteach agus dáta athbhreithnithe na heisceachta a shainiú i REG12 roimh cheadú na heisceachta.

9.1.5 [Both] Ní mór don System Owner / Application Owner eisceachtaí slándála PII atá imithe in éag a leigheas, a athnuachan nó a dhúnadh i REG12 laistigh de chúig lá gnó tar éis dul in éag.

9.1.6 [Processor] Ní mór don Vendor / Procurement Owner eisceachtaí slándála próiseálaí nó fophhróiseálaí a dhéanann difear do PII custaiméara a thaifeadadh i REG08 agus REG12 roimh ghlacadh.

10. Forfheidhmiú

10.1.1 [Both] Ní mór don Privacy Lead / PIMS Manager neamhchomhréireachtaí maidir le fianaise slándála PII atá in easnamh nó neamhiomlán a thaifeadadh i REG12 laistigh de chúig lá gnó ón sainaithint.

10.1.2 [Both] Ní mór don Information Security Lead úinéireacht leigheasúcháin le haghaidh teipeanna rialaithe slándála PII a shannadh i REG12 laistigh de chúig lá gnó ón mbailíochtú.

10.1.3 [Both] Ní mór don System Owner / Application Owner rochtain PII neamhúdaraithe, iomarcach nó gan tacaíocht a dhíchumasú nó a shrianadh laistigh de lá gnó amháin ón mbailíochtú agus an gníomh a thaifeadadh i REG12.

10.1.4 [Conditional] Ní mór don Incident Response Coordinator gníomhartha forfheidhmithe a nascadh le REG10 laistigh de lá gnó amháin nuair a bhaineann an t-ábhar forfheidhmithe le teagmhas PII amhrasta nó deimhnithe.

10.1.5 [Both] Ní mór do Top Management athbhreithniú a dhéanamh ar neamhchomhréireachtaí slándála PII athfhillteacha nó ardriosca i REG12 roimh athbhreithniú bainistíochta.

11. Athbhreithniú agus cothabháil

11.1.1 [All] Ní mór don Privacy Lead / PIMS Manager athbhreithniú a dhéanamh ar an mbeartas seo leis an Information Security Lead ar a laghad go bliantúil agus toradh an athbhreithnithe a thaifeadadh i REG12.

11.1.2 [Both] Ní mór don Information Security Lead athbhreithniú a dhéanamh ar bhonnlíne slándála PII i REG12 laistigh de 30 lá tar éis athrú ábhartha teicneolaíochta, bagartha, iniúchta, teagmhais nó rialála a dhéanann difear do shlándáil PII.

11.1.3 [Both] Ní mór don System Owner / Application Owner fianaise slándála PII ar leibhéal córais a nuashonrú i REG12 laistigh de 30 lá tar éis athrú ábhartha ailtireachta, rochtana, cumraíochta, leochaileachta nó logála.

11.1.4 [Processor] Ní mór don Vendor / Procurement Owner athbhreithniú a dhéanamh ar fhianaise freagrachta slándála PII próiseálaí agus fophhróiseálaí i REG08 laistigh de 30 lá tar éis athrú ábhartha seirbhíse, treorach custaiméara nó fophhróiseálaí.

11.1.5 [All] Ní mór don Internal Audit / Compliance Reviewer fianaise athbhreithnithe beartais agus fianaise roghnaithe rialaithe slándála PII i REG12 a fhíorú de réir an phlean iniúchta cheadaithe.

12. Beartais ghaolmhara

12.1 Ba cheart an beartas seo a léamh in éineacht le:

12.1.1 PII01 - Beartas um Chóras Bainistíochta Faisnéise Príobháideachais;

12.1.2 PII02 - Beartas um Rólanna, Freagrachtaí agus Cuntasacht Príobháideachais;

12.1.3 PII03 - Beartas um Fhardal Próiseála PII agus Bonn Dlíthiúil;

12.1.4 PII07 - Beartas um Measúnú Riosca Príobháideachais agus DPIA;

12.1.5 PII08 - Beartas Príobháideachais de réir Deartha agus de réir Réamhshocraithe;

12.1.6 PII09 - Beartas um Bhailiú, Úsáid, Nochtadh agus Comhroinnt PII;

12.1.7 PII10 - Beartas um Choinneáil, Scriosadh agus Diúscairt PII;

12.1.8 PII12 - Beartas Bainistíochta Príobháideachais Próiseálaithe, Fophhróiseálaithe agus Tríú Páirtithe;

12.1.9 PII13 - Beartas um Aistriú Idirnáisiúnta PII;

12.1.10 PII15 - Beartas um Bainistíocht Teagmhas agus Sáruithe PII;

12.1.11 PII16 - Beartas um Oiliúint, Feasacht agus Inniúlacht Príobháideachais;

12.1.12 PII17 - Beartas um Fhaisnéis Dhoiciméadaithe agus Bainistíocht Fianaise PIMS;

12.1.13 PII18 - Beartas um Fhaireachán, Iniúchadh agus Feabhsú PIMS.

13. Caighdeáin agus creataí tagartha

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].