|  |  |
| --- | --- |
| **Eàrr-ràdh 32B** | Appendix 32B |
| **Bristeadh a thaobh Dàta pearsanta** | **Personal Data Breaches** |
| Tha an GDPR a’ fàgail **dleastanas** air a h-uile buidheann gus aithris a dhèanamh air cuid a sheòrsaichean bristidh a thachras a thaobh dàta, far am feum iad innse mu dheidhinn don ùghdarras stiùiridh fhreagarrach, agus uaireannan, don Neach dham Buin an Dàta a chaidh a bhristeadh.Tha bristeadh air dàta pearsanta a’ ciallachadh gun deach tèarainteachd a bhristeadh agus gun deach dàta pearsanta a mhilleadh, a chall, atharrachadh, fhoillseachadh gun chead, no gun d’ fhuaras cothrom air gun chead, air thuiteamas no ann an dòigh mhì-laghail. Tha sin a’ gabhail a-steach bristidhean a thachair air thuiteamas no ri linn rudeigin a rinneadh a dh’aona-ghnothach, leithid, coimpiutair, tablet, stob-cuimhne no faidhle pàipeir a chaidh a chall no a ghoid. No a’ faighinn fiosrachadh tro fhoill bho làraich-lìn, puist-d no faidhlichean eileagtronaigeach. Faodaidh e cuideachd a bhith a’ ciallachadh a’ co-roinn fiosrachadh gun chead no ann an dòigh neo-iomchaidh, me, a’ cur post-d le fiosrachadh dìomhair no pearsanta chun an neach cheàrr.Faodaidh bristidhean air dàta pearsanta a bhith a’ gabhail a-steach:* neach gun chead a’ faighinn cothrom air;
* gnìomhan a rinn (no nach do rinn) rianadair no neach-làimhseachaidh a dh’aona-ghnothach no air thuiteamas;
* a’ cur dàta pearsanta chun an neach cheàrr;
* ma thèid uidheaman coimpiutaireachd le dàta pearsanta a chall no a ghoid;
* ma thèid dàta pearsanta atharrachadh gun chead; agus
* mura h-eil dàta pearsanta ri fhaotainn tuilleadh.

Faodar bristeadh air dàta pearsanta a mhìneachadh ann an dòigh fharsaing mar thachartas co-cheangailte ri tèarainteachd a bheir buaidh air cho dìomhair no iomlan ’s a tha dàta pearsanta no air mar a tha e ri fhaotainn. Gu h-aithghearr, bidh bristeadh air dàta pearsanta ann uair sam bith a thèid dàta pearsanta a chall, a mhilleadh, fhoillseachadh no a dhèanamh coirbte; ma gheibh neach cothrom air no ma bheir iad seachad e gun chead ceart; no mura h-eil an dàta ri fhaotainn agus gu bheil sin a’ toirt droch bhuaidh nach beag air daoine.*Mar sin, chan eil bristeadh dìreach a’ ciallachadh gun deach dàta pearsanta a chall.***Ma bheir sibh an aire do Bhristeadh air Dàta Pearsanta feumaidh sibh:*** Innse do (CUIRIBH ANN AINM AN NEACH LE UALLACH AIRSON SEO) agus don mhanaidsear agaibh sa bhad. Bu chòir dhuibh post-d a chur gu (CUIRIBH ANN AINM AN NEACH LE UALLACH AIRSON SEO) air (CUIRIBH FIOSRACHADH CONALTRAIDH AN SEO) agus cuideachd bu chòir dhuibh fònadh thuca air (CUIRIBH AN ÀIREAMH AN SEO). Feumaidh sibh sin a dhèanamh taobh a-staigh 72 uairean a thìde bho thug sibh an aire don bhristeadh, mas urrainn dhuibh. Mura h-eil (CUIRIBH ANN AINM AN NEACH LE UALLACH AIRSON SEO) ann seach gu bheil iad dheth, bu chòir dhuibh fios a chur gu (CUIRIBH ANN AINM AN DÀRNA NEACH LE UALLACH) air (CUIRIBH FIOSRACHADH CONALTRAIDH AN SEO).
* Nì (CUIRIBH ANN AINM AN NEACH LE UALLACH AIRSON SEO) co-dhùnadh an uair sin feuch am feumar innse don FCO mun Bhristeadh. Às bith dè an co-dhùnadh a bhios aca, innsidh e/i mu dheidhinn don Bhòrd (NO DON LUCHD-RIAGHLAIDH FHREAGARRACH AIG A’ BHUIDHINN AGAIBH) agus thèid clàr a chumail de gach bristeadh ann an oifis Inbhir Nis.
* Ma tha e buailteach gu bheil cunnart mòr gu bhith ann gun toir am bristeadh droch bhuaidh air còraichean is saorsa dhaoine, innsidh (CUIRIBH ANN AINM AN NEACH LE UALLACH AIRSON SEO) do na daoine sin sa bhad.
* An uair sin, thèid ath-sgrùdadh a dhèanamh air gach modh-obrach airson dìon dàta airson dèanamh cinnteach nach tachair a leithid a-rithist.
* Thèid trèanadh a chur air dòigh, ma tha sin a dhìth.
* Modhan-obrach airson Bristeadh air Dàta aig (CUIRIBH AINM NA BUIDHNE AN SEO) CEANN-LATHA
* Cuideachd, cumaidh (CUIRIBH AINM NA BUIDHNE AN SEO) clàr de bhristeadh sam bith air dàta pearsanta, co-dhiù a dh’fheumar no nach fheumar fios a chur chun an ICO.
* Bu chòir do luchd-obrach eòlas a chur air a’ Phoileasaidh airson Dìon Dàta agus am Poileasaidh airson Dàta nach eilear a’ Cleachdadh Tuilleadh.

**Liosta-dhearbhaidh**Ag ullachadh gus dèiligeadh ri bristeadh air dàta pearsanta* + Tha fios againn air mar a dh’aithnicheas sinn bristeadh air dàta pearsanta.
	+ Tha sinn a’ tuigsinn gu bheil bristeadh air dàta pearsanta a’ gabhail a-steach barrachd air dìreach suidheachaidhean nuair a thèid dàta pearsanta a chall no a ghoid.
	+ Tha sinn air plana gnìomh ullachadh gus dèiligeadh ri bristidhean air dàta pearsanta a thachras.
	+ Tha sinn air dleastanasan a bhuileachadh air neach fa leth no sgioba gus dèiligeadh ri bristidhean.
	+ Tha fios aig ar luchd-obrach air ciamar a dh’innseas iad do neach no sgioba freagarrach sa bhuidhinn againn mu dheidhinn tachartas co-cheangailte ri tèarainteachd, gus dearbhadh an deach dàta a bhristeadh.

A’ dèiligeadh ri bristeadh air dàta pearsanta.* Tha pròiseas againn gus measadh a dhèanamh air a’ chunnart a tha buailteach a bhith ann do dhaoine mar thoradh air bristeadh.
* Tha fios againn air cò th’ anns an ùghdarras stiùiridh fhreagarrach airson nan gnìomhan a nì sinn gus dàta a chur gu feum.
* Tha pròiseas againn gus fios a chur chun an ICO mu bhristeadh taobh a-staigh 72 uairean a thìde bho fhuair sinn a-mach mu dheidhinn, fiù ’s ged nach eil am fiosrachadh uile againn mu na thachair.
* Tha fios againn air dè am fiosrachadh a dh’fheumas sinn a thoirt don ICO nuair a tha bristeadh ann.
* Tha pròiseas againn gus innse do dhaoine air a bheil bristeadh a’ toirt buaidh nuair a tha e buailteach gum bi cunnart mòr ann gun toir e buaidh air na còraichean is saorsa aca.
* Tha fios againn gum feum sinn innse do dhaoine air am faodadh am bristeadh buaidh a thoirt gun dàil.
* Tha fios againn air dè am fiosrachadh a dh’fheumas sinn a thoirt do dhaoine mu bhristeadh, agus gum bu chòir dhuinn comhairle a thoirt dhaibh gus an cuideachadh le bhith a’ cur dìon orra fhèin bho bhuaidh sam bith a bheir e orra.
* Bidh sinn a’ cumail clàr sgrìobhte den a h-uile bristeadh, fiù’s ged nach fheumar aithris a dhèanamh orra.

Modhan-obrach airson Bristeadh air Dàta aig (CUIRIBH AINM NA BUIDHNE AN SEO) CEANN-LATHA. | The GDPR introduces a **duty** on all organisations to report certain types of personal data breach to the relevant supervisory authority and, in certain cases, the Data Breach subject.A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes, for example, the loss or theft of a laptop, tablet, memory stick or paper file. Or the hacking of websites, emails or other electronic files. It can also mean the unauthorised and inappropriate sharing of information that is personal eg: sending an email containing sensitive or personal information to the wrong person.Personal data breaches can include:* access by an unauthorised third party;
* deliberate or accidental action (or inaction) by a controller or processor;
* sending personal data to an incorrect recipient;
* computing devices containing personal data being lost or stolen;
* alteration of personal data without permission; and
* loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.*So it means that a breach is more than just about losing personal data.***If you identify a Personal Data Breach you must:*** Inform the INSERT RESPONSIBLE PERSON and your line manager immediately. The INSERT RESPONSIBLE PERSON should be emailed on INSERT CONTACT DETAILS and also telephoned on INSERT DETAILS HERE. You must do this within 72 hours of becoming aware of the breach, where feasible. If INSERT RESPONSIBLE PERSON is unavailable due to absence, INSERT SECOND IN LINE should be notified on INSERT CONTACT DETAILS HERE.
* The INSERT RESPONSIBLE PERSON HERE will then decide if the Breach needs to be reported to the ICO. Regardless of this, s/he will inform the Board (OR YOUR APPROPRIATE GOVERNANCE ARRANGEMENTS) and a record will be kept of all breaches by Inverness office.
* If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the INSERT RESPONSIBLE PERSON HERE will also inform those individuals without undue delay.
* All data protection procedures will then be reviewed to ensure no repeat of this incident. Training will be arranged if necessary.
* Data protection security should be a routine part of everyone’s daily work.
* (INSERT NAME OF ORGANISATION HERE)Date Breach Protocol DATE
* (INSERT NAME OF ORGANISATION HERE) will also keep a record of any personal data breaches, regardless of whether we were required to notify ICO.
* Staff should familiarise themselves with the Data Protection Policy and Abeyance Policy.

**Checklist**Preparing for a personal data breach☐ We know how to recognise a personal data breach.☐ We understand that a personal data breach isn’t only about loss or theft of personal data.☐ We have prepared a response plan for addressing any personal data breaches that occur.☐ We have allocated responsibility for managing breaches to a dedicated person or team.☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.Responding to a personal data breach* We have in place a process to assess the likely risk to individuals as a result of a breach.
* We know who is the relevant supervisory authority for our processing activities.
* We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
* We know what information we must give the ICO about a breach.
* We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
* We know we must inform affected individuals without undue delay.
* We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
* We document all breaches, even if they don’t all need to be reported.

(INSERT NAME OF ORGANISATION HERE) Date Breach Protocol DATE. |