NORTHERN IRELAND POLICING BOARD

POLICY ON DATA PROTECTION RESPONSE MANAGEMENT

This document, introduced in May 2018, sets out the Board's policy and procedure for handling requests for personal information in line with data protection legislation requirements.[1]

1 Process for Handling Subject Access Requests

Allocation and Acceptance

All requests for personal information are co-ordinated and managed by the Board's Communications Branch.

If you receive a request for personal information you must pass it to the Communications Branch Records Management staff **immediately**. The Records Management staff will allocate the request to the relevant Information Asset Owner (Director) within 2 working days.

Where input is required from more than one branch a single IAO will be asked to take the lead, in the event of confusion or dispute about the allocation of a request, the case will be escalated after 3 working days to the Chief Executive as the Senior Information Risk Owner (SIRO) for arbitration.

Request Compliance timescales

An individual (Data subject) who applies for their personal data (in writing or verbally) under the DPA is entitled to a response to their request within ***28 calendar days*** from the date of receipt of proof of identification – See Appendix A for more details about this.

If proof of identification is required please contact the Records Management staff who will request this from the individual.

Request timelines may be extended (which is new under DPA) where they are "complex or numerous", for up to a maximum of 56 calendar days. If you think this will be required you must always seek advice from the Records Management Team, as it is only available in certain circumstances. The individual requesting their information must be informed of this extension as early as possible, within the first 28

[1] On 25 May 2018 UK data protection law is changing, to ensure compliance with EU General Data Protection Regulation and the Law Enforcement Directive. Among a range of other changes, the timescale for responding to requests for personal data have been tightened, and individuals have been given several new rights. The new timescales are challenging, and will require prompt handling of requests to avoid ICO fines.

calendar days and provided with the reasons for such an extension. The Records Management Team will issue this information.

In most circumstances personal data must be provided free of charge. However, a 'reasonable fee' can be applied to cover administrative costs when a request is either "manifestly unfounded or excessive". You must always seek advice from the Records Management Team as this is only available in certain circumstances.

Finally, where there is a large quantity of personal information held about an individual, clarification can be sought from the individual in relation to what data specifically their request relates. Please seek advice from the Records Management Team before you issue a clarification letter to the data subject.

Monitoring Points and Escalation

After allocation and distribution to the IAO request owner, the first reminder will be triggered **10 calendar days** from the receipt of the request and confirmation of the requester's identification (if necessary). The reminder will take the form of a formal notice to the IAO request owner giving details and asking for the request to be expedited urgently or the reasons clearly stated why they feel this is not possible. This reminder will be sent by the Records Management Team.

The second and final reminder will be triggered **25 calendar days** from receipt and is considered a 'red flag' notification as it highlights that only the promptest action will now prevent the Board being in breach of compliance and at risk of adverse publicity or enforcement action by the Information Commissioner. This will take the form of a formal notice to the IAO owner, asking for the request to be expedited immediately or the reason for non-compliance stated. The formal **25 calendar day** reminder will be sent by the Records Management Team and copied to the Chief Executive as the Senior Information Risk Owner (SIRO) highlighting the risk to the Board.

Should a case reach the **28 calendar day statutory deadline** without an authorised extension, the Records Management Team will formally escalate it to the Chief Executive as Senior Information Risk Owner (SIRO). The SIRO will contact the relevant Director highlighting the breach of statutory timescales and risk of ICO penalties. This letter will give notice that the Board is now in breach of the Data Protection Act, and unless **immediate action** is taken, the case will be reported to the Board's Data Protection Officer (DPO) and recorded as part of the Chief Executive's report to the Board.

2 Other Rights based requests

The new Act gives individuals the right to make four new types of request:

a. The right to rectification
b. The right to erasure
c. The right to restrict processing
d. The right to object

These have the same statutory timescales and will be managed in the same way as Subject Access Requests. The relevant IAO will be advised by the Records Management Team at the outset should the request cover any of these rights.

3 Complaints

Data Protection legislation now allows dissatisfied applicants to complain directly to the Board's Data Protection Officer. These complaints will be logged by the DPO and should they relate to a subject access request or other data subject's rights, will contact the relevant team(s) and IAO as part of their independent review of the request management processes.

All complaints will be recorded by the Board's DPO and reported to the Chief Executive. Any unresolved complaints, will be escalated to the Board Chief Executive for a final decision as the Data Controller.

4 Appeals

Information Commissioner's Office

An individual (Data Subject) has the right to appeal directly to the Information Commissioner's Office as the independent regulator in the UK.

It should be noted that the ICO's powers under DPA are much greater than those under FOI Act. For example, if they are dissatisfied with any aspect of a case, including time compliance, internal processes or the quality of the response, the ICO has the power to conduct regulatory audits and/or impose undertakings or **civil monetary penalties/fines of up to €20m**.

Information Tribunal

Should either the individual (Data Subject) or the Board as Data Controller disagree with the ICO's findings/action, they each have an independent right of appeal to the Information Tribunal (UK High Court).

Appendix A

Confirming the requester's identity (Extract of guidance provided by the ICO)

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that you know the identity of the requester.

You can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on their behalf).

The key point is that you must be reasonable about what you ask for. You should not request a lot more information if the identity of the person making the request is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

Example

You have received a written SAR from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your organisation's policy is to verify identity by asking for a copy of a utility bill, it would be unreasonable to do so in this case since you know the person making the request.

However, you should not assume that, on every occasion, the person making a request is who they say they are. In some cases, it is reasonable to ask the person making the request to verify their identity before sending them information.

Example

An online retailer receives a SAR by email from a customer. The customer has not used the site for some time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, before responding to the request it would be reasonable to gather further information, which could be as simple as asking the customer to confirm other account details such as a customer reference number.

The means by which the SAR is delivered might affect your decision about whether you need to confirm the requester's identity. For example, if a request is made by means of an email account through which you have recently corresponded with the requester, you may feel it is safe to assume that the SAR has been made by the requester. On the other hand, if the request is made via a social networking website, it would be prudent to check it is a genuine request.

The level of checks you should make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.

Example

A GP practice receives a SAR from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requester is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for more information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious. They could ask the requester to provide more information, such as a document providing evidence of date of birth or passport.

Before supplying any information in response to a SAR, you should also check that you have the requester's correct postal or email address (or both). If you are supplying information by fax (and we recommend that you do so only if the requester specifically asks you to), then you must ensure that you are sending it to the correct fax number.

Trim 350117

Appendix B

Data Protection Response Management Timeline