CHARITIES INSTITUTE IRELAND

Information and Guidance Notes
General Data Protection Regulation (GDPR)

Article 30 - Data Inventory/Data Mapping

General Data Protection Regulation (GDPR)Information Notes - Article 30 – Data Inventory/Data Mapping.

Introduction

More than ever, the General Data Protection Regulation (GDPR) brings the issue of the protection of personal data centre stage. The GDPR requires charities/NfPs (Controllers) to ensure the security of personal data entrusted to them. It requires that the personal data held by your charity/NfP be documented, to indicate where it comes from, where it is transferred to and how it is secured throughout its life cycle.

But how to comply with these new requirements when a charity/NfP is not in a position to know what data they hold? The proliferation of data sources and the complexity of the applications' landscape in which data circulates (business applications, software packages, data management tools, mobile applications etc) complicate the tracing of the data path. (*If data and processes in your charity/NfP can directly or indirectly identify the data subject (individual/natural persons), this data and processes are viewed as 'Personal Data').*

Within the regulation there is an emphasis that all personal data must be easily contained and that each charity/NfP must have a system in place to monitor on a permanent basis the different operations carried out on personal data. To do so requires charities/NfPs to have a register of activities. The GDPR requires charities/NfPs not only to be able to identify and protect data wherever they own it, they are responsible for the accuracy of data they hold. (*To be aware, legacy data is often a prime candidate for housing out-of-date information).*

To implement the regulatory requirement of the GDPR charities/NfP's must first identify and locate this data in their systems and outline what processing it is subject to. This is called data mapping and is necessary to document (keep records of) this information. So, if there is a project to start immediately as a prerequisite for the GDPR and the Office of the Data Protection Commission has recommended that charities/NfPs commence with Article 30 (Record of Processing Activities) it is data mapping. Without data mapping - a precise census of data, their processing, their flows, the components through which it circulates, the individuals who process the data, it is impossible for a charity/NfP to fulfil its requirements under GDPR. Critical to this is capturing details on the categories of; personal data, data subjects, purposes of processing, destination of data, accessing etc.

Article 30: Records of processing activities.

Each controller (charity/NfP) shall maintain a record of processing activities under its responsibility, including:

- Name and contact details of the controller (charity/NfP), and, where applicable, the joint controller, the controller's representative and the data protection officer
- The purposes of the processing
- A description of the categories of data subjects
- A description of the categories of personal data.
- Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
- Where applicable, transfers of personal data to a third country, including the identification of that third country and the transfer mechanism relied upon.
- Where possible, the envisaged time limits for erasure of the different categories of data
- Where possible, a general description of the technical and organisational security measures

Who is obliged to maintain a Record?

- Each controller (ie charity/NfP and, where applicable the controller's representative.

Exemptions:

- An organisation employing fewer than 250 persons **unless**

  The processing is likely to result in a risk to the rights and freedoms of the data subjects

  The processing is **not occasional**, or

  The processing includes special categories of data

  (Charities Institute Ireland would recommend that all charities/NfP's complete the requirements under Article 30).

How should a Record look?

- In writing including in electronic form. (The records must be in writing with electronic form also acceptable under the provisions of Article 30(3))
  See: Example 1- Records of Processing Activities

How to commence

Charities/NfPs should undertake a gap analysis as soon as possible to evaluate their data protection programme and the creation of a register referring to existing processes that manipulate 'personal data'. A simple spreadsheet can be used for this. This requires not only the mapping all 'personal data' within your charity/NfP, but also the channels through which your charity/NfP communicates with beneficiaries, donors, supporters etc., including privacy policies, website, contracts, newsletters, e-commerce tools, internal procedures in terms of data leakage.

The use of service providers (processors) is also a factor in the complexity of data mapping operations. It will require that all partners be identified and any treatments/usage of 'personal data' placed under their responsibility, as well as the contractual considerations governing the relationships be considered. Where Data Processor Agreements are not in place with these processors, they will need to be put in place to comply with the GDPR.

It can be difficult for charities/NfPs to identify all the providers (especially Cloud) to whom data is transmitted or entrusted. In this instance, you should confer with your IT team or providers who should be able to assist you. They may also use a remote Data Recovery site operated by a third-party host, who by the nature of their service will be deemed a third-party processor, and as such you will need to carry out due diligence on them as to their adequacy of protection of the personal data under your control.

After such an analysis, the measures that allows your charity/NfP to comply can be identified. There is 'no one size fits all' approach and your charity/NfP should conduct these exercises in a way that fits your charity's/NfP's culture. Make sure to receive support for this project and it is essential to identify who is heading it up and involve all staff who oversee the data processing chain, including IT, marketing, fundraising, finance, HR, services to beneficiaries etc. Identify roles and responsibilities before any work begins and determine what exactly you are mapping. Setting realistic expectations for the level of effort required to complete the project will keep it moving and on track.

It is necessary to start by making an inventory of all the data flows as well as the data processes undertaken by your charity/NfP. Each department needs to identify

- the types of data subject (individuals/natural persons) who interacts with their department, i.e., it can be employee, supplier, beneficiaries, donors, supporters etc.
- For each such category, it is necessary to identify the data collected.
- It is then necessary to identify the flows carrying these data from their point of capture to their point of treatment/usage.
- Then it is a question of identifying the processes associated with or applied to such data.

In other words, each department should be asking and documenting all the following to get a precise inventory of the data in their possession and what they do with it. (Please also see questionnaires and interview questions below).

- What personal data do you store?
- What data subjects does it pertain to? (Service users, donors, staff etc)
- Where it is stored?
- What are you doing with the data?
- How do you process it?
- What lawful basis do you have (are relying upon) to process this data?
- How and when did you get it?
- Volunteers who collect data for you. The who, the what, the where, the when and the how?
- When do you use it and when does the purpose for it end?
- Is there a business need for the data? (Is the information necessary?)
- Who has access to it and what do they do with it?
- How long do you keep it?
- Is it encrypted?
- What other providers do you share it with?
- Countries where you transfer data to?
- How is it deleted
- Etc.,

Decide How to populate your Data Map.

There are three methods how this can be undertaken:

- Questionnaires & Interview
- Data Discovery (Automated Scanning)
- API integrations (Feeds from other systems)

(For these notes, we will focus on questionnaires and Interviews)

Example of Questionnaire

Questionnaire Part 1

- What is the name of the system where data elements are collected, stored and shared?
- Who is the system owner?
- What is the name of the business function that uses the system? (e.g. fundraising, marketing, HR etc)
- Is this a business-critical system?
- What is the main purpose of the system (e.g. Email, marketing, etc)
- What is the type/functionality of the system? (e.g., device, server, directory, application, website, mobile app)
- Are access permissions set on the system to ensure people only have access to those areas they need to access?
- Who is designated as the system administrator responsible for granting access to the system?
- Who is the IT contact for the system?
- What is the physical location of the system's server? (city/country)
  Is the system hosted by your charity/NfP or a third party? (If third party, who)

Questionnaire Part 2.

- Does the system process personal data?

  (*Personal Data: Any information relating to an identified or identifiable natural person)*

  (Identifiable person: Someone who can be directly or indirectly identified including by reference to a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person.)
- Does the data include any of the following types of information?

  (Race, ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, unique biometric data, health data, data concerning sexual orientation and sexual activity. Data relating to criminal convictions or offences)
- Is PII (Personally Identifiable Information) transferred across national borders? (and, if so, from where to where)
- Is system access reviewed and what is the frequency of the review?
- Is a data retention policy followed for this system and what is the retention policy followed for this system and what is the retention period?

Questionnaire Part 3.

- Does this system receive data from or send data to an external third-party, including third-party hosts? (if so, from/to whom) (Is third party use of data covered by a written contract?)
- What internal systems feed information into this system?
- What internal systems receive information from this system?
- Is there any role or department based privacy training conducted for individuals? If so, with what frequency and is there documentation?
- If the system where breached, what would be the anticipated consequences?
- Is there a data breach or incident management policy in place?

Interviews – 5 W's (Why, Whose, What, When, Where)?

- Why is personal data processed? (e.g. Donor relationship management, direct marking activities, HR administration, Legal obligations, etc.)

For each reason for processing:

- Whose personal data is processed? (Recipients of services, donors, staff etc)
- What personal data is processed?

  …… (Identify type of personal data, including:

  (Personal Details: *name address, email telephone, DOB, race ethnicity etc. Financial details – bank account credit card details, tax ids etc, health information, IP addresses, Employment details etc. source of the data – Individuals, third party individuals (processors/volunteers) other including social media, public records etc.*

  …… (And the legal basis for processing;

  Personal Data: *consent, legitimate interests, public interest, vital interest, compliance with legal obligation, performance of contract*.
  Sensitive Personal Data: *explicit consent, legal obligations relating to employment, vital interests, charity/NfPs, Public Information, legal claims, substantial public interest, healthcare/medical purposes, public health, archiving/scientific research.*

- When is personal data processed? (*When is personal data obtained/updated? What disclosures occur, to whom, and in what circumstances? How long is data retained and what determines the retention period?)*
- Where is personal data processed? (*Manual records location, electronic records format(s), systems/Services used. How is personal data protected, what controls exist?)*

Example 1 - Records of Processing Activities

			Content of the Record (Controll					
			[name and address of controller]					
			Responsible for this Record of Processing Activities:	[Insert name and contact details]	Name of Data Protection Officer (if any):	[Insert name and contact details]	Name of Data Protection Representative (if any):	[Inse cont a
		MANDATORY FIELDS IN RECORD						
Department (Fundraising, HR, IT)	**Name of IT System Software**	**If applicable, name and address of joint controller**	**Work stream**	**Information owner**	**Purpose for processing**	**Categories of Data Subjects**	**Approximate volume of Data processed**	**Cat e da**
			Fundraising - Donor information	Head of Fundraising	Processing donations, fundraising asks, campaigns and events, donor care, surveys	Donors, volunteers	Depends on number of contacts on database	Nam addr num detai for age num
			HR payroll	HR Manager	Staff payroll	Staff provide HR with relevant information (e.g. bank details, address) HR input staff details into HR system HR use 3rd party to process payments	500 staff records	Nam hom detai Natio num num

er)							
rt name and ct details]							

OF PROCESSING ACTIVITIES ACCORDING TO ARTICLE 30 OF THE GDPR

gories of Personal ta processed (list types)	**Categories of Recipients/Disclosees**	**Data location (hard and soft copies)**	**Basis for processing (legal/operational/marketing)**	**Where is data sent ? Include 3rd Countries.**	**Adequate safeguards relied on for 3rd countries.**	**Retention Period**	**General description of technical and organisational security measures**
e, address, email ess, phone bers, bank account ls, personal reasons onating/fundraising, ange, PPS bers,	Fundraising team, finance dept, 3rd parties - printers/agencies			Printers, agencies in Ireland. Use of survey tools - Surveymonkey etc, data stored in US cloud	Contracts	varies depending on data. PPS numbers needed for end date on CHY4 form + 12 months for processing	Password protection of data files, encryption of laptops, secure ftp file transfer to 3rd parties, clean desk policy, password protect PCs
e, email address, address, bank ls, salary details, nal Insurance ber, contact ber.	HR Admin staff,department of social protection, pension adminstrators			Jurisdictions where processed?	BCRs, Model Clauses, Consent?		

Charities/NfPs need also to be attentive to:

- Data received or exchanged with Partners. It is crucial not to neglect the consideration of service providers and suppliers (including volunteers) and it is necessary to cross-reference the list of service providers/suppliers of your charity/ NfP with the flows and processing of 'personal data' It will be necessary to ensure that you have identified personal data received from partners, sent to partners and/ or partners who have access as part of the services provided to your charity/NfP.
- Hunting Wild Places. Beyond official and current processes and applications, there are also ancillary treatments, implemented discreetly or which are no longer in use but where personal data can still be present. It is necessary to also look for them during the construction phase of the mapping.
- Maintenance. Maintaining and updating mapping is an important objective. This objective must be achieved by implementing appropriate processes. One way is to feed the mapping update based on established and systematic processes for projects that modify information systems. It will be a requirement under the GDPR to integrate personal data issues into the early stages of the life cycle of IT, marketing, fundraising and service project (risk analysis, needs analysis, etc.). (Privacy by Design and Default and Privacy Impact Assessments, Articles 25 and 25 respectively.)

CHARITIES
INSTITUTE
IRELAND