NYMITY INSIGHTS

Does GDPR Article 30 require a Data Inventory?

Teresa Troester-Falk
Global Privacy Strategist

Paul Breitbarth
Director, EU Certification Research
and Senior Solutions Advisor

July 2017

Many privacy officers seem to be under the impression Article 30 of the General Data Protection Regulation (GDPR) on records of processing activities, creates a legal obligation for traditional data inventory or data mapping exercise. This is not the case. The GDPR replaces current EU legal obligations requiring you to notify and register your processing activities with local data protection authorities (DPAs). Under the GDPR, you are no longer required to make such notifications but rather are required to maintain a record of all your organisation's processing activities internally, and to make them available to supervisory authorities upon request. Just as you had an external register, you now need an on-demand internal record[1]. The existing requirements vary by country with some countries requiring more information than others. Organisations compliant with this requirement, will have this information readily on hand and it should not be difficult to pull together the Article 30 record quickly.

How is a data register (processing data inventory) different from a traditional data inventory? Let's begin by looking at what comprises a traditional data inventory.

Traditional Data Inventories

A data inventory is a record of the data assets that an organisation handles and can cover both personal data or general data (accounting, statistical data, network data, etc). General data inventories are typically driven out of the IT, security, or governance department through manual or automated tools and include details on the network and infrastructure. These records often do not contain details on personal data elements or personal data processing activities. On the other hand, personal data inventories, generally motivated by privacy management program initiatives, attempt to record detailed information on the nature of organisation's data holdings (e.g. HR data, customer data or sales data). It is focused on the "repository" or "silos" for the data and is classically formatted in a tabular or Excel-based format and through automated solutions.

For privacy management purposes, the fields in the record can vary from organisation to organisation but typically include the following[2]:

- The nature of the data holding (e.g. Human resources data)
- The owner of the data holding
- Location of the data holding
- The volume of information in the data holding
- The format of the information (Paper or electronic? Structured or unstructured?)
- The use of the information
- The data elements (e.g. name, physical address, email address, government identifier, health information, salary information)
- Where the data is stored (in which country/countries)
- Where the data is accessed (from which country/countries)
- International transfers (data flows – country by country)
- The record can help identify which data is most and least

[1] The requirement does not apply where the controller employs fewer than 250 persons and the processing is not likely result in a risk for the rights and freedoms of data subjects, is occasional, or is not of special categories of data (which means most organisations will be caught)
[2] Adapted from "Elements of a Data Inventory", Privacy Program Management, An IAPP Publication, 33.

Pros and Cons of Starting Your GDPR Program with a Data Inventory

Privacy officers are often taught that the first step in establishing a privacy program is to create a personal data inventory as way of prioritizing efforts, resources, assessing risks, and preparing for privacy incidents and breaches. Many suggest this is also the first step in assessing gaps for GDPR compliance. Looking at the above list, it is easy to see how this could be helpful. Logically, until an organisation truly understands what personal data they have, where it is located, and how it moves through and out of the organisation, it is not possible to protect it nor is it possible to fully comply with the GDPR (at least in spirit). Yet for those who have attempted such exercises through the years, either manually or through automated solutions, they know this is a resource intensive challenge. It is difficult to know if all the data was truly inventoried and it soon becomes evident that it is not possible to maintain such an inventory. Further, Nymity research has been unable to identify a single successful data inventory managed by the privacy office that has lasted for over three years. Automated solutions motivated solely for privacy compliance have failed over time).

> *The privacy office is dealing with a moving target because the data an organisation holds is almost constantly changing, without notice - the larger the organization, the more complicated and complex the exercise.*

Furthermore , data holdings inventories do not align with how the business works. Consider a single data holding that contains a variety of personal data. That data holding (or a component of it) might have multiple processing activities – it may be processed for marketing purposes, used to fulfill and deliver a product for someone who orders a product from an online store and may also be used by your finance department for regulatory reporting purposes. There may be different retention periods for each, associated with the purpose. From a data holdings inventory perspective, all of this would need to be recorded. Because of this complexity, data holdings inventory efforts are often incomplete and attempts to perpetually maintain the inventory are almost always abandoned. All data holdings inventories created and maintained solely for the purposes of privacy compliance are inaccurate either at the time of creation or soon thereafter.

Is the effort a waste of time? No. There are still good reasons to create a snapshot in time of data holdings if one has the budget and resources to do so.

The data inventory provides the critical information while the focus of the privacy office becomes less on the labour-intensive task of ensuring the inventory is perfectly maintained, and more on creating policies and procedures to ensure that personal data is appropriately processed and protected on an ongoing basis, throughout the organisation.

Whether an organisation decides to devote resources to this traditional and extensive exercise or not, the GDPR provides an opportunity to approach data inventories in a new way.

A Processing Data Inventory and the GDPR

Having looked at the nature of a traditional personal data inventory (a data holdings inventory), let's turn our attention to a data processing inventory. This concept may appear new but, as noted above, for organisations operating in the EU, a requirement of the EU Data Protection Directive 95/46/EC was to notify and register processing activities with local DPAs. Article 30 replaces this requirement and in this context, a processing data inventory is the same as a "records of processing activities" register. The French data protection authority (CNIL) recently published a 6-step methodology for complying with the GDPR[3] which includes an Article 30 template . This template further highlights that a traditional data inventory is not the intent of Article 30.[4]

In general, these records must contain:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer ;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

It is important to note this list is first concerned with *the details of processing activities versus the details of a data holding repository* and does not require the onerous process of documenting every data element that forms part of the data repository (though in practice, some companies may still want to do this).

The Benefits of a Data Processing Inventory

A data processing inventory reflects how the business processes data and starts with listing the processing activities and their purpose. Why is this significant and how does it impact the organisation? A data processing inventory is aligned with how the business works making it is easy for the business to engage and the Privacy Office getting more and better data.

More and more organisations are transitioning their data inventory efforts to a processing data inventory because it makes sense and aligns with how the business works.

[3] www.cnil.fr/fr/comment-se-preparer-au-reglementeuropeen-sur-la-protection-des-donnees
[4] www.cnil.fr/fr/cartographier-vos-traitements-de-donneespersonnelles

As Oran Kiazim, Vice President, Global Privacy at Sterling Talent Solutions has stated, a data processing inventory is first "about the how and the why, the 'where' is secondary." Consider an internal process for background screening of employees. There may be several data holdings impacted. If the Privacy Office asks the HR department to identify the repositories of personal data and the details of each holding involved in the background screening process, the business often will not know. To satisfy the request, the business must engage in a time-consuming effort to gather the data. This may result in incomplete or even inaccurate information provided to the Privacy Office resulting in the business giving up. However, if the Privacy Office asks the HR department, "what data do we process for criminal background checks", this is information the business can easily provide.

GDPR Article 30 and Processing Data Inventory

The GDPR creates an opportunity for organisations to limit their data inventory to just an inventory of their data processing operations, instead of all their data holdings. For example, consider an initiative involving the processing of personal data for benefits and payroll. Many privacy and data protection professionals will already have this information at hand. Putting together an Article 30 record may be quite straightforward. For other organisations with less mature privacy management infrastructures, pulling this data together will require some work. In all instances, taking a data processing inventory approach to Article 30 requirement vs. a data holdings inventory will be much more efficient.

Some suggest in order to properly address data subject rights such as access, erasure and portability requests under the GDPR, a data inventory is critical. However, it is important to note that the access, correction and deletion requirements have existed for decades under data protection laws across the globe. Organisations have been effectively addressing and responding to these requirements despite not having a personal data inventory in place. After the basic details of Article 30 requirements are met, organisations may choose to add more detail to their record.

There may be good reasons to record the specific data elements and the location of the data even though this is not required by Article 30. So, the outcome of approaching the data inventory this way results in the same information being captured, but the inputs are designed in a way that aligns with business process.

How to Make a Data Processing Inventory Work

As stated above, maintaining a data inventory motivated by privacy compliance is impossible. A processing data inventory needs to be an outcome of a larger initiative. For example, some organisations have risk reviews for every project. If the right information is incorporated into the risk review process, the review will obtain the necessary information for a data processing inventory including meeting the obligation in Article 30 GDPR). Another possibility is to obtain the necessary information during a security review. The challenge with taking these approaches is they won't capture processing that does not involve the implementing of new software solutions for the purposes of, for example, marketing campaigns and employee surveys.

Nymity's research has resulted in delivering an approach where the business is motivated to conduct project reviews with the primary motivation being speed rather than privacy compliance. Nymity's solution ultimately enables the business to do more processing of personal data, enabling the business to easily identify similar purposes and to incorporate that learning and data into new processing operations. Businesses can use legitimate interest as legal grounds for processing including processing current data already collected from past processing as well as finding data, and repurposing it with demonstrable compliance.

Nymity's solution enables the business to demonstrate compliance and to do more processing while reporting the benefits that the business is providing to the individuals for whom data is being processed. In fact, the business can demonstrate mitigation of potential harms to the individual and risks of processing the personal data. The business conducts project reviews for their own gains and the solution produces a data processing inventory in which the business might not even know or care they are doing so. In short, the business does more and the privacy office is provided a Processing Data Inventory that produces GDPR Article 30 records of processing activity reports and much, much, more.

About Nymity

Nymity is the leading global research company specializing in accountability, risk, and compliance software solutions for the privacy office. Nymity's suite of software solutions helps organizations attain, maintain, and demonstrate data privacy compliance. Organizations all over the world rely on Nymity's software solutions to proactively and efficiently manage their privacy programs - empowering them to comply with confidence. For more information visit www.nymity.com.