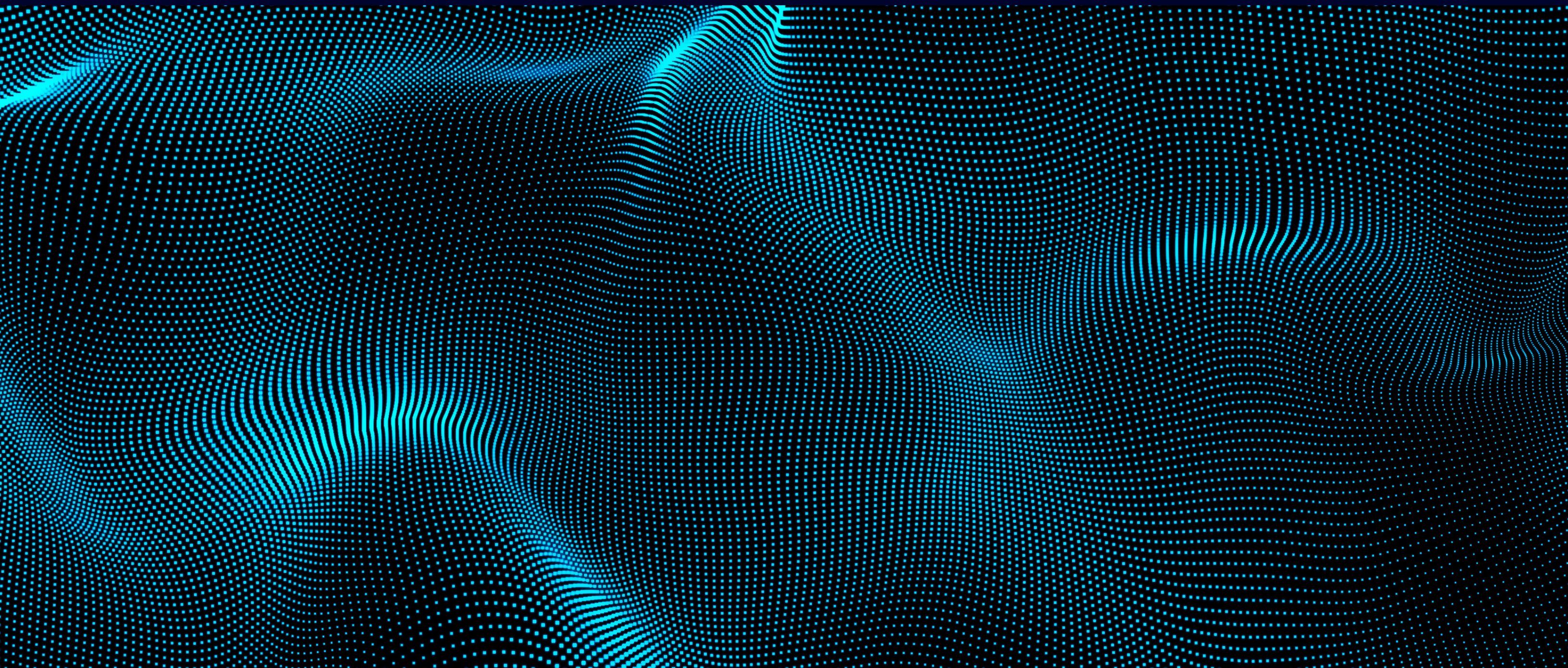
WHITE PAPER

RELYANCE AI

How to Get the Most Out of Your Records of Processing Activity Using Regulatory Guidance and Better Tooling

Records of Processing Activities (ROPAs) are a fundamental component of a compliant data protection program, yet often, they are the most onerous. Learn how the right approach to ROPAs can allow you to crack the code of Data Protection Boards and add a new risk-management tool to your arsenal.



Background

While the initial record of processing activity (ROPA) was created as a means of meeting regulatory requirements, if done right, ROPAs can be used as a strategic tool to understand and manage processing activities and help to get a handle on data across your organization. The General Data Protection Regulation 2016/679 (GDPR) introduced a number of groundbreaking data protection requirements, not the least of which was the requirement that controllers and processors[1] maintain Records of Processing Activities (ROPAs). Established in Article 30 of the GDPR, the creation and maintenance of ROPAs has proven to be one of the most onerous data governance requirements for controllers and processors to meet. The UK Data Protection Act 2018 (UK DPA) and Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais or "LGPD"), impose similar obligations. While the UK DPA essentially served to apply to the GDPR to the UK post-Brexit, the LGPD differs in that its requirements are not as prescriptive as the GDPR[2]. Traditionally, developing a compliant ROPA required hours of research and time spent collaborating with data custodians and owners throughout an organization.

However, despite the effort required to maintain ROPAs, they are nonetheless a tremendous risk management tool and best practice for all organizations that process personal data. ROPAs offer additional benefits beyond promoting awareness of data use and good data governance across an organization; they can serve as a means of protecting your organization's data assets by providing clarity about how data flows to your vendors. This is particularly beneficial for organizations that engage a large amount of vendors to process their information–by understanding which vendors to monitor the most closely, you will reduce the likelihood of any vendor mishandling your data or failing to apply the appropriate security measures when processing it.

[1] Under GDPR Article 4, a "controller" is "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means" of its data processing operations. A "processor", on the other hand, is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". The definitions of each under the LGPD are similar.

[2] See LGPD Article 37.

In addition, ROPAs can provide insights into the priorities and expectations of regulators, as the Brazilian Data Protection Authority (ANPD)[3] and a number of Data Protection Authorities in the European Union and United Kingdom have published sample ROPAs and other guidance. These materials shed light on each regulator's expectations for both controller and processor ROPAs, which may become invaluable should your organization be subject to a regulatory audit.

This paper will examine how ROPAs are traditionally generated, discuss some of the guidance issued by Data Protection Authorities in the EU and UK, and provide suggestions for how organizations can leverage available tools to streamline and improve the ROPA process.

[3] Known officially as The Autoridade Nacional de Proteção de Dados or “ANPD.”

The State of ROPAs Today

Given the GDPR's prescriptive requirements for the content of ROPAs, it is no surprise that the compliance process has proven to be such a time and resource drain on organizations intent on complying with the law. Article 30 of the GDPR sets out a prescriptive list of the information that must be included in ROPAs generated by controllers and processors[4]:

- The name and contact details of the controller or processor, their data protection officer (DPO), and/or their representative[5] (controllers and processors)
- The purposes of the processing (controllers)
- A description of the categories of data subjects and the categories of personal data (controllers)
- A description of the categories of processing (processors)
- The categories of recipients the data is disclosed to (controllers)
- Any transfers of data from the EU to a third country (controllers and processors)
- Where possible, the data retention periods for various categories of data (controllers)
- A general description of the technical and organizational security measures used to safeguard the data (controllers and processors)

In practice, ROPAs are usually completed by a DPO or privacy team in collaboration with contacts throughout the organization. The workflow generally involves identifying and interviewing data owners in each business unit, as well as in internal services departments such as legal, who likely have additional information on the data types in the organization's inventory due to their need to be able to scope and implement litigation holds. Essentially, the DPO or privacy team will conduct a data flow analysis identifying the organization's data assets, the recipients of that data, and the way that data flows around the business and externally to the organization's vendors. This process can be extremely time consuming and prone to error, as the party responsible for managing ROPAs is subject to the responsiveness and accuracy of their associated teams.

[4] Controllers and/or processors may be exempt from the obligation to maintain ROPAs if such organizations employ fewer than 250 people, the processing it carries out is not likely to result in a risk to the rights of data subjects, is occasional, and does not include any special categories of data (set out in GDPR Article 9) or data relating to criminal convictions or offenses.

[5] GDPR Article 27 requires controllers or processors that do not have an establishment in the EU but that still come within the scope of the law to appoint a representative in the EU.

What Insights Can We Draw from the Available Guidance?

A number of Data Protection Authorities throughout the EU, UK, and Brazil have published guidance on ROPA best practices, often in the form of a sample ROPA template. Specifically, the ANPD and the Data Protection Authorities in the UK (ICO)[6], France (CNIL)[7], Germany (BFDI)[8], Belgium (APD-GBA)[9], Finland (ODPO)[10], Ireland[11] (DPC), Cyprus (CPDP)[12], and Poland (PUODO)[13] have each published sample ROPAs for controllers, while the ICO, BFDI, and ODPO have published sample ROPAs for processors as well. While the samples include the basic information required under GDPR Article 30 and share many similarities, particularly among the sample processor ROPAs, they provide a number of insights into the priorities and regulatory approach of various Data Protection Authorities.

By including data fields in their sample ROPA that are not strictly required under the GDPR, regulators apparently intended to illuminate the subject areas that they prioritize when monitoring compliance with the GDPR or LGPD. For example, a number of regulators want to see whether a controller has considered the risks their processing operations pose to the data subjects whose data they are processing. Specifically, the Brazilian ANPD and Belgian APD-GBA suggest that controllers detail the risks likely to result from their processing operations, with the Brazilian ANPD's guidance advises that controllers detail the results intended for the data subjects.

[6] The Information Commissioner's Office, "ICO."

[7] Le Commission Nationale de l'Informatique et des Libertés, or the National Commission on Informatics and Liberty "CNIL."

[8] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, or the Federal Commissioner for Data Protection and Freedom of Information, "BFDI."

[9] Autorité de la protection des données - Gegevensbeschermingsautoriteit, or the Data Protection Authority, "APD-GBA."

[10] Tietosuojavaltuutetun Tomisto, or the Office of the Data Protection Ombudsman "ODPO."

[11] The Data Protection Commission, "DPC."

[12] Επίτροπος Δεδομένων Προσωπικού Χαρακτήρα, or the Commissioner for Personal Data Protection "CPDP."

[13] *Prezes Urzędu Ochrony Danych Osobowych*, or the Polish Data Protection Commissioner "PUODO."

In addition, the UK's ICO, Irish DPC, Belgian APD-GBA and Cypriot CPDP all suggest that controllers note whether their evaluation of the risks to data subjects triggers the GDPR requirement that they conduct a Data Protection Impact Assessment (DPIA), and if so, to document the results of the DPIA[14]. Further, the UK ICO and the Irish DPC have suggested that, where applicable, controllers document their legitimate interests for processing personal data, and include their legitimate interests assessment[15]. Taken together, these suggestions illustrate that the applicable Data Protection Authorities want controllers to carefully consider the risks their processing operations pose to data subjects, and to conduct thorough assessments to establish whether those risks are sufficiently mitigated.

In addition, the sample ROPAs illustrate that virtually all of the Data Protection Authorities maintain a focus on the legitimacy of a controller's basis for processing personal data, particularly in the case of higher-risk processing operations. The UK ICO, Irish, French, Belgian, Cypriot, and Brazilian Data Protection Authorities each require that controllers document their legal basis for processing, particularly in the case where sensitive personal data is involved[16] while the UK ICO also directs controllers to note where the subject processing operations include automated decision-making, including profiling, which are prohibited unless the controller has a specific legal basis specified in the GDPR[17]. While these suggestions are not surprising given the risk-balancing approach the GDPR and LGPD prescribe, they reveal that a Data Protection Authority is likely to focus on whether an organization met the applicable legal requirement for whichever lawful bases they rely on.

[14] Introduced under Article 35 of the GDPR, a controller is required to conduct a Data Protection Impact Assessment (DPIA) where a type of processing is likely to result in a high risk to the rights or freedoms of data subjects. Article 36 requires a controller to consult with a competent supervisory authority prior to beginning the processing operation where the DPIA indicates that the processing would result in a high risk.

[15] Included in GDPR Article 6, one of the iterated lawful bases for processing personal data is where it is "necessary for the purpose of the legitimate interests pursued by the controller". In order to rely on the "legitimate interests" basis, a controller must balance whether those interests are overridden by the interests or data protection rights of the data subjects involved in the processing.

[16] Under Articles 4 and 5, respectively, the GDPR and LGPD generally define "sensitive personal data" as data concerning race or ethnicity, religion, union or political affiliation, health information, or data concerning one's sexual orientation.

[17] GDPR Article 22 provides that data subjects may not be subject to a decision based solely on automated processing, including profiling, which produces legal effects on the data subject, or otherwise similarly affects them, unless the processing operation is based on the data subject's explicit consent, authorized by EU or member state law, or is necessary for the performance of a contract.

Lastly, the available guidance can also serve to clarify ambiguities in the law. Specifically, the guidance issued by the ANPD is particularly interesting given that Article 27 of the LGPD does not specify what information must be documented by controllers or processors. In evaluating the published ROPA, it becomes clear that the ANPD intends for controllers and processors to generally conform to the basic requirements of the GDPR, including the documentation of the processing activities, categories of data subjects and personal data, description of technical and organizational security measures, data recipients and processors, retention period, and any international transfers of data. That approach makes clear that the ANPD expects controllers or processors subject to the LGPD to produce ROPAs in a similar fashion as controllers and processors subject to the GDPR.

Regulatory guidance and better tooling can make ROPA maintenance a more efficient, beneficial process.

As noted earlier in this paper, the current ROPA workflows suffer from a total lack of efficiency. As most privacy professionals will agree, the hours spent interviewing data owners and passing spreadsheets around the organization could be better spent doing any number of data governance tasks. While organizations familiar with the available guidance will have a head start in understanding regulator priorities and operationalizing their ROPA obligations, the act of gathering and organizing information about an entire organization's data inventory and processing activities is by its nature a time-consuming and resource-intensive process.

Unfortunately, most governance, risk, and compliance platforms available today fail to bring any efficiencies to the ROPA process. While some platforms may offer a convenient portal to create and store ROPAs, privacy teams are still left going through the tedious process of gathering information about their organization's processing activities, data inventory, and data flows.

Relyance AI is out to change that. The Relyance AI Platform leverages machine learning-based instrumentation and code, infrastructure, contract, and vendor integrations that provide you with an **automatically and continuously updated live data map and data inventory** that serves as the foundation for all of your privacy and data protection requirements, including the creation and maintenance of ROPAs.

Relyance AI builds out a live data map and data inventory in 4-5 hours, without requiring access to underlying personal data, that lets you and your team answer questions you didn't even know you had. Our proprietary Natural Language Processing (NLP) code runs through your data map and inventory and automatically generates ROPAs in the form published by any Data Protection Authority, with no manual intervention needed. At the click of a button, our platform will produce a ROPA in the format your regulator prefers.

Conclusion

By automatically creating your ROPAs in accordance with applicable regulatory guidance, the Relyance AI Platform will allow you to enjoy the benefits of well-crafted ROPAs and good data governance. Rather than devoting most of their time to ROPA development and upkeep, your DPO and/or privacy teams will be able to spend more of their time executing on the insights drawn from your ROPAs.

RELYANCE AI

The information provided on this paper does not, and is not intended to, constitute legal advice; instead, all information, content, and materials in this paper are for general informational purposes only. The information provided in this paper may not constitute the most up-to-date legal or other information. Readers should contact an attorney to obtain advice with respect to any particular legal matter.