Expedient

Author: Daniela M. Monte Serrat Cabella, CIPM

Zoox Smart Data

Notice: This material can be used to create derivative works, as long as the source and author are mentioned.
INTRODUCTION

A “Privacy Program” is, by the very definition of “program”, “a set of measures or activities related to a specific long-term objective”. A Privacy Program must present a structure that provides the basis for the privacy and data protection professional to act with confidence in order to orientate the organization to go beyond simple compliance with legislation and contribute to the common good. This structure should take into account any and all data protection legislation that affects the operation of the organization, and should incorporate privacy by design and by default approaches. When well implemented, it contributes to the organization’s management and longevity, greater operational efficiency and customer loyalty, and adds value to it, almost as a separate asset.

We live in a moment of transition to a new culture, of sustainable use of personal data. The implementation and continuous improvement of a Privacy Program so that this new culture becomes, in fact, a reality involves several activities and demands a great effort and investment from the organization. Being aware of the size of the challenge and its complexity, and having received several requests from customers and partners to share the structure of Zoox’s Privacy Program, we decided to publish a short version, in the form of a practical guide, to contribute to the market and facilitate the implementation of the same type of Program in other organizations as well.
PROGRAM MANAGEMENT

Ideally, the Management of the Privacy Program should be carried out by the Data Protection Officer (DPO) or Chief Privacy Officer (CPO), with the support of a team fully dedicated to privacy and data protection matters, and reporting directly to the organization's CEO. It is essential to ensure that, within the specific scenario of the operation, the Program Manager and the privacy and data protection team have:

1. Access to direct communication with the organization's strategic decision maker, ensuring that there is no “filter” nor “delay” (intentional or unintentional) in relation to communications regarding privacy and data protection;

2. Concrete autonomy to conduct the Privacy Program, and

3. Exemption from any conflicts of interest related to their position in the organization.
All the actions and activities of the Privacy Program must be guided by the seven principles of the Privacy by Design framework, created by Ann Cavoukian, which are:

I. Proactive not reactive: preventative not remedial

II. Privacy as the default setting

III. Privacy embedded into design

IV. Full functionality: positive-sum, not zero-sum

V. End-to-end security: full lifecycle protection

VI. Visibility and transparency: keep it open

VII. Respect for user privacy: keep it user-centric
OBJECTIVES

The objectives of Zoox’s Privacy Program are:

1. **COMPLIANCE** - To monitor and continuously improve the level of privacy and data protection compliance, propose measures to go beyond simple compliance with legislation and add value to the final consumer and the organization itself;

2. **RISK** - To perform privacy and data protection risk analysis and risk management in an effective way, in accordance with consolidated international best practices and taking into account ethical aspects involved in the processing of personal data;

3. **PRIVACY BY DESIGN** - To promote privacy by design and by default in the organization’s products and services;

4. **GOVERNANCE** - To elaborate, review, implement, disclose, update and monitor the level of adherence to data protection policies, standards and procedures, including those related to information security, in order to contribute for the organization to be ready to respond, in an efficient and timely manner, to any incidents with personal data, as well as to act and respond to requests from data subjects and public authorities, and

5. **COMMUNICATION AND CULTURE** - To contribute to the creation and strengthening of a privacy and infosec culture both internally as well as externally (market).
IMPLEMENTATION

Please find below the main activities to be conducted in order to ensure the efficiency of both the Program management and the implementation of each of the five objectives.

Foundation and Management

Appoint the organization’s CPO or DPO.

- Signature of the Appointment Letter with the description of the responsibilities, obligations, activities, guarantees and limitations of the function, as well as the coverage of its performance (group or organization only, national or international territory), to be signed by the CEO or equivalent function in the organization.

- Internal communication of the appointment. The ideal is to communicate both informally (which is usually more direct and effective) and formally (which documents the official communication).

- External communication, which must include the mentioning of who the DPO is at the organization’s website, as well as other forms of communication to the market and the authorities.
Ensure that Privacy and Data Protection are inserted as the Organization’s Values.

Ensure that Privacy and Data Protection are included in the Strategic Planning and become the organization’s “core” Strategies.

Insert privacy and data protection guidelines in the organization's Code of Ethics and Conduct.

Ensure that there are sufficient financial and human resources to perform the Program's activities (it is the organization's responsibility to provide such resources).

Implement a management system. Considering that the Program requires frequent contact with all areas of the organization and that they often request action from the DPO and the Privacy and Data Protection team, it is necessary to have an organized and structured way to receive and respond to such requests. It is recommended to use project management softwares such as Monday, Jira, Trello or Notion.

Apply agile methodology to manage the activities and requests related to the Program. There will always be a lot of work to do, so it is recommended to adopt one-week sprints and the matrices RUT and RICE to help prioritize the activities and actions in the backlog. In Annex I, there is more information about these matrices and their adaptation to Zoox’s Privacy & Data Compliance team workflow, made by Marcelo Martins, Scrum Master and Project Manager, and Daniela Cabella, DPO and Head of Privacy & Data Compliance.

Establish a Privacy and Data Protection interdepartmental Committee, with its own rules of procedure, for collective decision-making in relevant cases.
Compliance

Map all personal data and processing operations, both from the organization's products and/or services' users, as well as non-users, that is, employees, customer representatives, partners' representatives and suppliers' representatives, or other data subjects.

▷ Draw the operation flow, which can be done according to the ISO 29134 template or in a customized way.

▷ Create or review the personal data inventory and processing operations registration.

▷ Map the legislation applicable to the operation and the level of compliance for each legal control ("implemented", "documented" and "monitored", as in information security audits). The legal compliance control can be registered through the use of software, spreadsheets or in other forms - what really matters is to have an effective and complete control of the compliance level and to be able to extract data for decision-making and metrics to measure the Program’s evolution.

▷ For the compliance control regarding the Regulation no. 2016/679 (General Data Protection Regulation, or GDPR), there is an excellent control template published by the ICO, the UK’s Data Protection Authority (Information Commissioner's Office).
For the Brazilian General Data Protection Law (Law No. 13,709/2018, LGPD), it is important to adopt a control that covers it entirely. We adopted the Complete Privacy control template that aggregates all LGPD controls into five pillars (Foundations, Principles, Data Subjects’ Rights, Obligations and Governance) and adds to the Information Security control.

For the Information Security audit, it is recommended to adopt international best practices, such as the ISO 27001 or NIST frameworks.

It is important to document all activities that mean going beyond mere compliance and contributing to the common good.

Use the mapped controls to support decision-making activities and prepare Action Plans.

Map all existing contracts and carry out the inclusion or review of privacy and data protection clauses.

Develop, review or update standard data protection clauses, which should be customized for the organization’s business model.
It is possible to create models of clauses or Data Processing Agreements inspired by the Standard Contractual Clauses (SCC) that the European Commission has published or based on Data Processing Agreements publicly available (DPAs) from organizations recognized for their data protection efforts, such as ProtonMail, adapting them to local legislation (when applicable) and to the organization's business model.

Document technical and administrative measures that prove compliance with the seven principles of Privacy by Design.

Conduct audits (internal, in partners and in customers), to verify the level of privacy and data protection compliance that is applied throughout the personal data processing flow.
Risk

Establish a Risk Management program. There are several best practices and frameworks, and we adopted the ISO 31000 framework in conjunction with the seven principles of Privacy by Design.

Perform Privacy Impact Assessments (ISO 29134) and Data Protection Impact Assessment (DPIA) ICO.

Consider ethical aspects of the personal data processing activities as a measure that goes beyond mere compliance in risk assessments.

Analyze the need for hiring cyber insurance, and, if so, hire the most appropriate.
Privacy by Design

- Build support materials for the Product team (or equivalent), such as a Persona and User Journey with a privacy approach, to support the creation of new products, features or services which are privacy by design and by default.

- Integrate with the Product team (or equivalent) not only organically, but also in a structured way, creating processes and adopting tools that enable greater integration between this area and the DPO / Privacy and Data Protection team in the development of new solutions (products, features and services).

Governance

- Map which Policies (“guidelines”), Standards (“rules”) and Procedures for Data Protection and Information Security have already been developed, approved and communicated and which have not been developed yet. Use a support list, such as the example in Annex II.

- Prepare an Action Plan to write, approve, communicate, review and monitor compliance with all Data Protection and Information Security Governance documents.

Communication and Culture

- Create a Communication Plan that guarantees the frequency and efficiency necessary to develop the Program’s activities.

- Internal Communication Plan to raise awareness on privacy and data protection matters, as a compliance measure, as well as to mitigate human error and strengthen the organization’s culture in these aspects.
External Communication Plan, as a measure that goes beyond compliance. In Brazil, the specific data protection legislation is recent, which means that we need to contribute to (i) help the user or final consumer who are data subjects (in general, the society) to understand that they have gained new rights, what these new rights mean and how to exercise them, as well as to (ii) collaborate with the market sharing best practices, in order to raise the general level of applied knowledge about privacy and data protection in the entire market - a practice that not only values the organizations which do so, but also contributes to the sustainable use of personal data.

Establish daily communication between the DPO and the Privacy and Data Protection team to ensure alignment, agility and efficiency in carrying out the Program’s activities.

Establish direct communication with the CEO, at least weekly, to address Privacy and Data Protection matters.

Ensure that there is free and direct communication (also frequent) with all teams (managers and operations) to align Privacy and Data Protection matters.

Develop and apply semiannual, or more frequent, Privacy and Information Security training to strengthen the organization’s Data Protection culture, and measure (test) the level of content absorption. Develop an Action Plan to correct low absorption of specific content, if applicable.
CONTINUOUS IMPROVEMENT

The organization and the context in which it operates are constantly changing. Therefore, it is essential to maintain a PDCA cycle of continuous improvement. Some activities involved in this process are:

- Monitor the legislative scenario for new Bills related to privacy and data protection and which may affect the operation.

- Monitor the publication of new best practices for data protection.

- Determine the schedule for reviewing and updating data mappings, flows, inventories, policies, standards and procedures. Also review and update these documents in case of any changes in the business model or operation, or any changes in the corporate or legislative scenario.

- Conduct audits both internally and on suppliers, partners and customers.

- Develop a plan to ensure the continuous learning and evolution of the Privacy and Data Protection team.

- Make an effort to have both the organization and the professionals working with privacy and data protection matters certified.
FINAL REMARKS

Each organization can and should adapt the Privacy Program to its own business model and operation, always remembering to cover the five objectives to ensure that the Program is robust. Finally, it is important to remember that the Privacy Program documentation itself is already an administrative measure of Privacy by Design that complies with the principle of “proactive not reactive: preventative not remedial”, as well as the accountability principle.
ANNEX I

Agile Prioritization for Privacy and Data Protection Activities and Requests

By Marcelo Martins and Daniela Cabella

RUT Matrix

To apply the “Relevance x Urgency x Trend” (RUT) matrix to prioritize activities and requests involving the Privacy and Data Protection matters, we recommend that the Privacy Program Manager read each item on the backlog, clarify doubts if necessary, and invite all Privacy and Data Protection team members to vote (from 1 to 5), together with the Program Manager, each of the three criteria, as follows:

<table>
<thead>
<tr>
<th>VALUE</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relevance</strong> (What is the value for the Privacy Program?)</td>
<td>It is not part of the Privacy Program. It would be nice to have, but we were fine without it.</td>
<td>It is related to the Privacy Program, it would be nice to have.</td>
<td>Important for the Privacy Program.</td>
<td>Very important. The Privacy Program is not complete without this measure.</td>
<td>There is no Privacy Program without this measure.</td>
</tr>
<tr>
<td><strong>Urgency</strong> (What is the timing?)</td>
<td>Implementing now makes no difference. You can wait.</td>
<td>It is not good to be without it, but you can wait.</td>
<td>It is desirable to launch soon, in the next sprint perhaps.</td>
<td>We’ll be in trouble if it’s not on the next sprint.</td>
<td>It’s immediate. We cannot wait for the next sprint.</td>
</tr>
<tr>
<td><strong>Trend</strong> (What is the company’s perspective?)</td>
<td>The first impression is not good, but the company gets used to the absence of this measure.</td>
<td>It can be problematic for the company to continue without it.</td>
<td>It is certain that the company will be harmed without this.</td>
<td>The damage to the company is not only certain, it also increases over time.</td>
<td>It gets much worse every day, it is extremely exhausting for the company to continue without it.</td>
</tr>
</tbody>
</table>
Voting must take place at the same time (the famous “1, 2, 3, go!”) so that no one is influenced in their choice of grade. Most likely, there will be no initial consensus most of the time, and this will lead to an organized discussion about why each one chose a particular grade. The goal is for everyone to reach a final consensus on the grade for each of the three criteria and then multiply them. Thus, the score for each item in the backlog will be between 1 and 125 points, having the highest scoring points at the top of the backlog list (priorities) and the lowest scoring at the end (not a priority).

As Andressa Chiara points out in her article, there is great value in the discussions generated for the defense of the grades, as much information that emerges at that moment would hardly be revealed otherwise. In addition, it is possible to generate metrics of value delivered by sprint and added value, which, in our view, is also useful for the Privacy Program activities' and requests' management.

**RICE Matrix**

After assigning the RUT grades to the backlog items, it is common for some of them to have an equal score. As a tiebreaker criterion, we use the RICE Matrix (“Reach x Impact x Confidence x Effort”):

<table>
<thead>
<tr>
<th>Reach</th>
<th>Impact</th>
<th>Confidence</th>
<th>Effort</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics</td>
<td>1 to 5</td>
<td>%</td>
<td>People/ Sprint</td>
<td>A * I * C / E</td>
</tr>
</tbody>
</table>
Reach should be scored according to the number of people that the activity or task will impact (example: notification about updating the Privacy Policy for “X” users of the product); the impact level should be measured from 1 (low) to 5 (high); the confidence level of the Manager and the Privacy and Data Protection team should be measured in terms of percentage (the higher the percentage, the greater the confidence), and the effort should reflect the number of people involved in performing the task per sprint. The four criteria must be equated as follows:

\[(\text{Scope} \times \text{Impact} \times \text{Confidence}) / \text{Effort}\]

The resulting value should therefore be used as a tiebreaker for items with the same RUT score, meaning that those with higher RICE score should be prioritized over the ones with lower RICE score.
ANNEX II

List of Basic Governance Documents

- Information Security Policy
- Data Protection Policy
- Website Privacy Policy
- Products’ or Services’ Privacy Policies
- Risk Management Policy
- Information Classification Policy
- Identity and Access Management Policy
- BYOD Policy
- Cloud Computing Policy
- Remote Work Policy
- Password Policy
- Use of the Internet Policy
- Use of Wi-Fi Policy
- Background Check Policy
- Use of Public Social Network Policy
- Data Protection Training Policy
- Third Party Hiring and Auditing Policy
- PIA and DPIA Policy
- Personal Data Access and Use Standard
- Personal Data Transfer and Storage Standard
- Personal Data Retention and Deletion/Anonymization Standard
- Data Subjects’ Requests - Response Standard
- Authorities’ Requests - Response Standard
- Use of Information and Communication Technology Resources Standard
- Use of Cryptographic Controls Standard
- Incident Response Plan
- Business Continuity Plan
- Response and Notification Procedure - Data Subjects
- Response and Notification Procedure - Public Authorities
- Anonymization and Safe Deletion Procedure