Collibra

Whitepaper

# Practical steps for a customer-centric approach to data privacy

Many organizations are choosing to take a more customer-centric approach to the way they manage the personal data that they hold and use. They understand that a focus on the customer transforms data privacy into a business value driver.

According to a Forrester Consulting study commissioned by ForgeRock, 75% of organizations consider the safeguarding of customers' privacy to be a competitive differentiator and 79% say that safeguarding customers' privacy is a business priority. These organizations understand that customers are much more willing to engage with them  if customers trust them with their personal data.

75%

of organizations consider the safeguarding of customers' privacy to be a competitive differentiator

Building trust through a customer-centric approach to data privacy can generate a range of benefits for the business — it's a win-win scenario. Organizations trusted with consumers' personal data are better at obtaining new customers and retaining existing ones. They find it easier to build communities of customers who engage with their brand. This, in turn, translates into customers feeling more positive towards the brand overall, adding to the brand's value as an asset.

Taking a customer-centric approach to data privacy also builds trust within the organization around the use of personal data. Confidence and trust in personal data are increasingly necessary for organizations that want to take advantage of emerging technologies like AI and ML.

Conversely, failing to take a customer-centric approach to personal data can hold organizations back. For example, in the same Forrester study, 57% of respondents reported that their senior management fears AI and IoT will expose customers, including their personal data, to greater security and privacy threats. Additionally, 44% agreed that this fear leads to greater resistance toward further AI and IoT deployments. Senior managers are afraid of the financial and reputational damage that misuse of customers' personal data, or a data breach, could inflict on their organizations.

The good news is that all organizations can take a practical, Data Intelligence-led approach to making this goal a reality. Below are five key actions that organizations can take today to build a proactive and sustainable approach to customer-centric data privacy management.

## Transparency and control basics

- Strong internal policies around personal data
- Clearly written terms and conditions for consumers
- Automated tools for consumers to give them control over their personal data
- Processes and technology to operationalize policies and controls
- Training for all employees on personal data policies, with specialized training to support specific roles, such as marketing

**1. Provide transparency and control to consumers** – As mentioned earlier, consumers are more likely to do business with organizations they trust to handle their personal data in an ethical and secure manner. In this way, trust translates into business value and increased revenues. An important part of establishing this trust is providing transparency to consumers about what the organization intends to do with the consumer's personal data and providing control to consumers over the organization's use of their personal data. According to a recent survey by the UK's DMA, transparency is an important precondition for consumers who are deciding whether or not to share their data. The survey said that:

- 88% of respondents indicated that transparency about how their data was collected and used is important to them when sharing data with an organization
- 87% said it is important that the terms and conditions are easy to read and understand
- 85% said it is important for the organization to have a flexible privacy policy that allows them to control the types and amount of data they wish to share

To engage in the right way with consumers, it is important to get transparency and control basics right. This involves having a clear vision for the organization's culture about the "who, what, when, where, why and how" of personal data. For example, whose personal data is being used, what is it being used for and how is it being used? Organizations need to know this so that they can translate their policies into action — collecting and using personal data in the right way. Within the data governance discipline, the answers to these questions are known as the data lineage. It is almost impossible to provide consumers with real transparency and controls without operationalizing the lineage of the organization's personal data.

**2. Embed accountability** – An important ingredient within a relationship of trust is responsibility, and it is important for organizations to have a strong culture of accountability around its data. Policies should make it clear that employees are fully answerable for the way personal data is handled. To support this, the data governance program needs to entrench accountability within its overall operational framework. Ways in which it should do this include:

- Assign roles and responsibilities for personal data to employees across the entire personal data lifecycle, eg., who is responsible for the creation of a type of personal data – also known as the data owner

- Ensure there is a good reason for personal data to be collected in every case. The organization should not collect data "just because" it can – it needs to be accountable to consumers for the use of their personal data.
- Create a secure environment for personal data by restricting who has access to it, eg., individuals should only have access to personal data if they need it to perform their jobs
- Implant a culture of accountability around personal data through training, eg. employees who have access to personal data should learn how to handle data correctly, and the consequences of failing to do so.

In addition to instilling the culture of accountability among employees and creating detailed processes around how individuals handle data, an organization should also automate the processes that help maintain transparency. This is essential because attempting to manage accountability manually through spreadsheets and other task-focused tools leaves the door open for human error. Accountability policies and processes should align with the organization's overall data security program and its risk appetite for loss events such as data breaches, for example.

Ultimately, the organization — and its employees — are answerable to the consumers whose personal data they are using. Getting this right means that the culture of accountability needs to be supported by policies, processes and the right operational approach. The outcome of this should be stronger overall data governance and security, which is essential to building trust with consumers.

**3. Embrace privacy by design** – Privacy by design means considering data privacy and security from the beginning of any project, including the creation of new products and services. The concept of privacy by design has been around for a long time, but the EU's General Data Protection Regulation (GDPR) popularized the term by making it a requirement. However, this requirement should be viewed as an asset rather than an impediment.

Historically, some organizations have brought in data governance team members only at the end of the product development process. This "bolt on" approach to data governance and security leads to significantly increased risks such as:

- Data breaches or other data security issues
- Negative customer experiences, for example, where poor quality personal data can be directly encountered by customers

- Operational risks, for example, not having adequate personal data processing capabilities in the back office
- Poor product performance, such as when sub-standard personal data quality causes unexpected outcomes in AI and ML technology applications

As mentioned earlier, worries about these kinds of issues hold back organizations from engaging with AI, ML and IoT programs.

Today, organizations around the globe are adopting the privacy by design approach. According to the Forrester survey, 80% of businesses said that security and privacy considerations are built in from the start when developing new products, services and apps. Talking about data privacy and security at the beginning of projects just makes sense. It is much easier to get data privacy and security right if issues and challenges are discussed at the beginning, particularly for those that use AI, ML or IoT.

By taking a more considered and proactive approach to personal data privacy, organizations are driving more value from their projects. Consumers are much more likely to trust products and services that have a well-thought-out approach to data privacy and security woven into them. They are also more likely to trust organizations known for their ethical approach to delivering products and services. This trust translates into real business value through increased revenues, improved customer retention and successful marketing programs, for example. In short, using a privacy by design approach is just good common sense for organizations, whether it is an explicit regulatory requirement or not.

**4. Play by the rules** – If one thing is for certain, the number and scope of data privacy rules is set to grow. Back in May 2018, the EU's GDPR became the first big package of rules with which many global organizations had to comply. Now, individual states in the US are following suit and are passing data privacy legislation. The California Consumer Privacy Act (CCPA) — deadline January 1, 2020 — has received a lot of attention. Washington state, New York state and numerous other US states have their own laws in the works, while at a federal level Congress is hammering out its own nationwide privacy law. Then, there are the data privacy laws that are cropping up internationally — including in Bahrain, Brazil, Chile, India and New Zealand.

It is fairly obvious that an organization that wants to be trusted by consumers to handle their personal data must be fully compliant with any data privacy and security rules. However, the number of new data

## Thinking in a "privacy by design" way

- What kinds of personal data does a project require?
- In what ways will the project use the personal data?
- Is this kind of data collected at the moment? If no, what is needed to collect and process this data in an ethical way?
- If the project is using personal data the company already holds, how high is the quality of this data? What is its lineage?
- Is new investment needed for this project's personal data operations?
- What are the risks associated with this kind of use of personal data and how can they be mitigated?
- How will this project be transparent to and provide controls for consumers?
- Are there other ways in which the ethical use of personal data could add value to this project?

privacy laws being created — and the pace at which they are appearing — is generating real headaches for organizations, particularly since many of these laws have extraterritorial elements to them. As well, the laws differ from each other in fundamental ways, from scope of application to the rights with which they empower consumers.

Surviving — and thriving — in this kind of a regulatory environment requires a strategic approach that transforms compliance into a core part of the organization's ethical culture. Key actions include:

- Scan the regulatory horizon for data privacy rule changes, particularly in jurisdictions that the organization operates within. Don't be caught unaware.
- Bake regulatory change capabilities into the overall data governance framework
- Build best practices for policies and processes rather than a specific set of rules, so they are less likely to need adjustments in the face of new regulations
- Communicate regularly with the board and senior management about the impact of rule changes on the organization's strategic goals
- Add value by helping the business understand regulatory change and the way it will affect day-to-day activities

Getting regulatory change right — being nimble enough to adapt quickly and with minimal operational disruption to new rules — should be a key goal for all data governance programs. By ensuring that the organization is resilient in the face of regulatory change, the data governance team adds significant value overall, and ensures that consumers view the organization as a trustworthy corporate citizen.

**5. Respond the right way** – The truth is, when it comes to data privacy and security, risk events are likely to materialize no matter how hard an organization works to get it right. In part, this is because of the nature of the threat. Cyberattacks are happening more often, and these criminals yearn for customers' personal data. There is also the possibility of personal data being compromised from inside the organization — for example, cases of internal fraud or human error. If not handled in the right way, personal data breaches can significantly weaken the trust that customers have in the organization. Even worse, it can foster the perception that the organization is not ethical — that it did not properly secure customer data or that it created products that used personal data in improper ways.

As a result, it is important for organizations to be prepared for these events. In fact, the financial services regulators and the industry are focusing on improving preparedness for events such as cyberattacks and data breaches. This new focus, called "operational resilience," aims to put in place measures that reduce the impact of a negative event on the organization and its customers. Key action items for data breach resilience include:

- Understand the nature of the compromised data. When there is a data breach, it is important to be able to quickly identify who owns the data, how it is used in business processes, and what kind of personal data may have been accessed
- Report the breach within the timeframe required by any applicable regulators. To do this, it is important to know details about the data involved, such as which jurisdictions it has been used in. It is also important to have clear, automated processes for breach reporting — organizations need to ensure that deadlines are adhered to and that all compliance requirements are met
- Include operational resilience within contracts for third parties who handle the organization's personal data. For example, add language to contracts that require third parties to adhere to the organization's personal data policies. Another best practice is to include language that enables the organization to audit the third party's levels of compliance with these policies. Also include specific requirements for what needs to happen in the event of a data breach at the third party that involves the organization's data, such as breach reporting timescales and processes
- Create templates for communication with key stakeholders such as regulators, customers and employees, in the event of a data breach. By drafting communications documents in advance, it is possible to ensure that the documents are articulated correctly, and are compliant with any applicable regulations

## Resilience is not optional for survival

Operational resilience is the ability of an organization to prevent, respond to, recover and learn from operational disruptions to survive and prosper, and not cause harm to customers and the wider market.

– EY

An organization's prioritization of data privacy impacts consumer and stakeholder perception. However, one data incident does not define an organization's reputation; it is important to remember that an organization's responsiveness such incidents impacts its brand. One study by Deloitte showed that 59% of consumers agreed that a single data breach would negatively impact their likelihood of buying brands from a consumer products company. Nonetheless, the same study showed that 51% of consumers would be forgiving of a consumer products company that had one single data breach of their personal data as long as the company quickly addressed the issue. Companies with strong reputations for handling personal data well — who have built up high levels of trust — are much more likely to have resiliency in their relationships with consumers.

In short, it is important for an organization to take a more customer-centric approach to the way they manage the personal data that they hold and use. Organizations that adopt this strategy will be able to transform the relationship of trust that they build with customers into real business value for senior management, the board and shareholders. That is because having a strong reputation for personal data privacy and security makes organizations more trusted by consumers. In turn, consumers are much more likely to want to engage with these organizations.

Discussed above are tangible actions that an organization can take to build such a reputation. Actions do speak louder than words, but, as a final point, it is crucial to put in place a robust communications strategy with consumers, investors, regulators and other stakeholders around data privacy and security. Such a communications program should help make stakeholders aware of the actions that the organization is taking, as well as the benefits of those actions. A steady rhythm of communications helps to build a reputation for trustworthiness over time. Seeing the benefits of a customer-centric approach will not happen overnight — it can take time. However, the business value generated is well worth the investment in a more intelligent approach to personal data management.

**For additional questions, contact us at:**

| United States | United Kingdom | All other locations | By email |
|---|---|---|---|
| +1 646 893 3042 | +44 203 695 6965 | +32 2 894 79 60 | info@collibra.com |