A JITTERBIT WHITEPAPER

General Data Protection Regulation: The DPO's Guide to Compliance

Ensure Your Customer's Privacy is Secure and Maintain GDPR Compliance with Jitterbit

Table of Contents

Jitterbit

Overview

Regulation 2016/679 for the European Union, also known as General Data Protection Regulation, and even better known as GDPR, took effect on May 25th, 2018. For many companies and organizations worldwide, May 25th was also the day they began making efforts toward compliance to GDPR. That also means on May 25th, some individuals learned they now had the additional professional title of Data Protection Officer (DPO).

Being appointed the DPO for your company or organization doesn't mean you now work two full-time jobs. In fact, with the right tools and support at your disposal, achieving and maintaining compliance is easily attainable and manageable.

The most important thing is to address all requirements and necessary actions related to GDPR and avoid being put into a situation of non-compliance fines that can reach in excess of 10 million dollars or 2% of your worldwide yearly revenue from the previous financial year, depending on which is higher. Or even worse, it can damage your reputation beyond repair, affecting bottom lines not just for the EU market, but globally.

The DPO's Checklist

If you look at the individual areas of concern for GDPR, bringing attention and proportional effort into addressing that data privacy issue is enough to comply. To use a slightly antiquated analogy for today's modern world, if you had a checklist on a clipboard as you toured the landscape of data privacy across your company, you could probably check off most items in a day. You just need to know what you're looking for.

But we are in the modern world and there are solutions and technology to help you get them all checked off. Just take a look at how an API integration platform can help.

As an organization, Jitterbit has made certain that we have appropriate measures in place to meet our specific GDPR obligations as well as the needs of our customers. And Harmony, our enterprise integration platform as a service (EiPaaS) is an ideal solution for managing data, monitoring access points and end points, outbound communications and reporting across your entire global data footprint.

The following sections share key parts of how we scaled our implementation efforts with regard to GDPR and make for a great checklist for any DPO starting the project of becoming GDPR compliant.

1. Privacy-by-design

Connecting customer data across multiple systems is crucial to organize today's best of breed applications and services, but this modernized way of data-sharing and automation becomes complicated with GDPR requirements. For example, if an EU citizen opts to delete personal data shared with a company through one application, that company must ensure that the data is also removed from all other integrated applications and systems that had access to it.

The introduction of the concept Privacy-by-design is a change that must be adhered to with GDPR. Privacy-by-design is an obligation in which organizations must consider privacy at the initial development stages for all data processing. This concept is not new but is a legal requirements under the GDPR. It will be essential for your organization to understand the importance of privacy from the start of the development process.

- Jitterbit has implemented appropriate technical and organizational measures and procedures to ensure that data processing safeguards the rights of the data subject (by design) and that we process only personal data that is necessary. Whether you are a solution or service provider, starting at your core offering is essential.
- Jitterbit has always regarded privacy as a critical part of our corporate social responsibility (CSR) efforts. This is reflected in our internal standards, ethics, and public commitments. That commitment and transparency is important, and now a requirement with GDPR for contractual language and notifications.
- Implementing privacy-by-design can also result in organizational and procedural changes such as designating a privacy point person for procurement of new IT services
- Jitterbit's enterprise iPaaS enables companies to track GDPR-sensitive data across multiple systems, by ensuring that personal data can be tracked and accounted for at all times. Because Jitterbit users can granularly select the specific records and types of data to exchange between different applications or services, and get a clear visualization of how data flows across the enterprise, Jitterbit makes it easier for companies to comply with some of the more complex GDPR requirements.

2. Privacy-by-default

Privacy-by-default is when a system or service incorporates options for an individual as to how much personal data they share with others, and gives them the ability to control that data. As with privacy-by-design, privacy-by-default is not a new concept but is a legal obligation under the GDPR. Understanding privacy requirements from the beginning of the design process is critical in ensuring you approach the issue successfully. Knowing what data you want to use, and giving data subjects preferences on how their information will be used by applying privacy by-default principles, will also enable data control by the subject. There will not be any hidden information or surprises and trust can be earned.

At Jitterbit we understand transparency is critical in developing trust in regards to collecting customer data.

Here are a few examples of what you should work into your privacy-by-default design.

- Knowing where your data is and how it is exchanged between solutions is critical. It would behoove you to reduce the amount of places data is stored and keep processing of personal data to a minimum. Using Jitterbit, you can manage data from any single interface and user, such as your with your role as DPO.
- Evaluate the risks of reidentification by ensuring that data is anonymous and cannot be linked to the data subject. And find the right method for anonymizing data that fits your solution or service is important.
- Strong encryption, authentication and access control should be a major requirement and knowing who has access to subject data when and how they access it, and what they will be doing with the information is essential in maintaining compliancy and protecting your employees when performing their jobs. Your staff should be educated so they understand specific parameters in handling the data in accordance with GDPR regulations.
- Include the location of data in your development process. It is imperative that you understand what type of data you have and where the data resides. It is a key factor in staying compliant with the GDPR. With Jitterbit you can easily monitor data residency, integrity and flow across all connected systems.
- Implementing privacy impact assessments for all new applications

3. Risk Analysis and Risk Management

Formalized risk management is the cornerstone of any security program. Most organizations already have risk analysis programs as part of their standard IT initiatives. So is risk management. What is key around GDPR compliance is ensuring these elements aren't only the realm of IT departments, but implemented across the entire company in regards to data management. Developers need to understand data residency and processing only the necessary data. Marketers need to ensure data capture forms or even physical exchanges during conferences or trade shows comply to GDPR standards.

Jitterbit's process includes a combination of technical and non-technical methods including annual penetration testing, vulnerability assessment and management and 3rd party attestation for regulatory and standards compliance. The outputs of this process define the technology, process, and talent roadmap.

4. Administrative, Technical and Physical Safeguards

As just mentioned regarding marketing departments, data can be acquired in many different manners. Collecting business cards, electronic scans of trade show visitors, product trial users, advertising, all of these need to have safeguards built around how data is managed. Plus, the communication of data privacy and security along with transparency of how the data will be handled on top of properly conveying that the data subject controls how that data will be handled is important.

Jitterbit has implemented reasonable and appropriate safeguards in place to meet specific GDPR requirements, protecting confidential information.

Contractual language

Everyone has contracts – Our contracts are straight forward and easy to comprehend, as there are no surprises. It is simply effortless to conduct business with Jitterbit.

Data breach notification practices

Jitterbit understands it is our obligation to report within 72 hours. Knowing this we have developed and put in place a master breach notification plan, which includes the mandated reporting steps for every relevant regulation allowing us to report any reportable breach without undue delay.

Data flow

Data is only stored and processed (transient) for the minimum amount of time necessary to allow for the customer-intended processing. Because data and logs are in limited locations, it is easier to facilitate compliance with certain subject's rights.

Data subject rights

GDPR is about personal data protection. If you don't know where to access the data you have or the type of data you have gathered, remaining compliant will prove to be difficult. Under GDPR, the individual's data in which your company collected are allowed to request that it be changed, handed over to them or entirely deleted.

At Jitterbit, we understand the rights of those individuals whose data has been collected. We facilitate our own and your compliance with each one of them.

A few subject rights include:

Total Access to information

This right provides the data subject with the ability to access, view, modification and exporting personal data (about him or her) and understand e rationale for processing the data

Withdraw of consent

The subject has the ability to withdraw given consent for processing their personal data for a purpose. The company would need to stop processing the subject's personal data that was based on consent given at a previous time.

Erase Collected Data

Also known as right to erasure, this right provides the subject with the ability to ask for their data to be deleted. This could happen in a situation where a customer relationship has ended.

5. Extraterritorial compliance

Data residency is essential to GDPR. The data of EU subjects must reside in the EU, even if it is a cloud solution. That can be difficult to define with some cloud solutions, but necessary to stay in compliance.

The benefit of dealing with an organization that has a global footprint like Jitterbit is that we can host your data in the appropriate region; Jitterbit will never move the data for the region that it originates in. We have fully independent clouds for EU and non-EU geographies to ensure data on the platform will not be exposed across regions without client authorization.

6. Inbound Data Capture Channels

It is an adjunct of privacy-by-default for any data subjects. From the moment they share personal data, it needs to be handled within GDPR guidelines. And they need to retain control of how it is handled and if it should be "forgotten" completely by an organization.

Jitterbit requests subjects to perform simple, informed opt-ins to receive communications. Subjects can easily unsubscribe to selected or all communications at any time. Synchronization of customers' opt-in consent flows seamlessly between various business systems ensuring all subject information is current and collected in real-time.

Policies and procedures

Internal

Our internal policy-set defines the workforce behavioral boundaries for all sensitive data and forms the basis for our awareness campaigns

External

Jitterbit's privacy policy provides detailed information regarding how our company collects, uses, discloses and maintains subject data and exceeds their GDPR needs

7. Privacy Impact Assessment (PIA)

A PIA is a risk assessment of proposed processing of personal data. If your organization processes personal data that could result in a high risk and compromise a data subject's rights, your organization will need to conduct a PIA prior to processing the data. This is especially important when introducing any new systems or workflows in the any data management processes.

This goes along with the risk management and assessment that is taken on internal data processes and externalizing that approach. In essence, taking the view of the data subject and discovering if the process is likely to result in a high risk to the rights and freedoms of natural persons. If there is any concern here, a PIA is needed.

8. Training, Education and Awareness

Once we identified the extent of the GDPR in regards to our organization, we then needed to ensure our customers and internal teams had a clear understanding of how the GDPR's requirements affect the way we processed personal data. We extended our corporate privacy training to educate employees and partners about impending privacy regulations that could affect how we maintain compliance.

Although many organizations will need to adjust the effort around this, the focus should be to make the effort to ensure all are educated. Again, using ourselves as a model, Jitterbit does the following:

Our internal GDPR training include:

- Internal webinars, online training courses, and reference materials to train our employees on the GDPR's requirements, privacy obligations and security regulations.
- Train-the-trainer programs where subject matter experts led specialized trainings in their specific business divisions.

Our external GDPR training include:

- Technical and privacy documentation for our customers, detailing our compliance with GDPR, along with guides to help allow secure and compliant use of Jitterbit services and products.
- Webinars such as Five Key Elements for Every GDPR Plan are designed to keep our clients informed about how to leverage Harmony Cloud for compliant success.

9. Empowering DPOs

The importance of the Data Protection Officer is more than title alone. That is something that is not lost on us. Jitterbit has two dedicated professionals, one for the US and the other for the EU. They are well positioned in the company to ensure they can support and evolve the Data Protection Program; these individuals work with all levels within the organization in order to execute from the top down and bottom up.

The most important empowering factor for a DPO is the ability to view and manage all data, for integrity, residency and transactional security, quickly and across all systems. And when needed for reports and notifications, a means to customize and automate it all.

Conclusion

With each item above being addressed, and your role as a DPO overseeing them, your worries about GDPR should fade away. And with all data processing technology being connected by an integration platform, you can feel confident that you'll stay in compliance into the future.

The Jitterbit Harmony integration platform helps simplify the collection of your valuable customer data, providing a secure, 360° view of vital information so that both individuals and organizations can benefit from the digital economy whilst remaining compliant. Learn how Jitterbit can help your company remain compliant with GDPR and contact a solution expert for a personalized consultation by emailing us or calling +1.877.852.3500.