LEARN MORE

The GDPR Compliance Checklist

The General Data Protection Regulation (GDPR) takes effect on 25 May 2018 across the world to protect the privacy rights of people from the European Union (EU). The new regulatory regime governs how businesses and government institutions must handle the sensitive personal data of EU citizens, and levies substantial fines on organizations that fail to comply.

It is important for companies outside of the EU to understand that GDPR may still apply to them. You are subject to GDPR regulations if you acquire, control and/or process any personal data belonging to EU citizens, regardless of where you are headquartered, including the Americas, Africa, the Middle East, the Asia-Pacific region, and European countries that are not part of the EU.

Meeting GDPR requirements will force most companies to upgrade their IT infrastructure and services in areas like data protection, storage, networking and security. Compliance will also require the development of many new policies and procedures that employees and partners will have to be trained on and then execute scrupulously.

For many businesses, the path to GDPR compliance will be a long one. Given that the deadline is approaching fast, Acronis recommends a few concrete steps you can take immediately to start improving your GDPR compliance posture:

1

Learn the basics of GDPR jargon. At a minimum you need to understand what regulators mean by the terms personal data, data subject, data breach, controller, processor, supervisory authority, and the right to be forgotten. There are many more, but those are an essential starting point on your road to compliance.

2

Identify your company's role in the GDPR taxonomy of EU citizens vs. the companies that directly or indirectly handle their personal data. Are you a controller (an entity that acquires and handles personal data), a processor (a third party that processes personal data on behalf of a controller, e.g., the controller's cloud storage service provider), both, or neither?
For example, in GDPR parlance, Acronis is both a controller and a processor. We are a controller to our EU customers that buy backup and other application software from us: in taking their orders, providing them with customer service, and interacting with them in other ways, we acquire some of their personal data, including name, address, phone number and email address.

Acronis is also a processor as defined by GDPR: we own a global network of data centers that our partners use to offer cloud-based backup-as-a-service, cloud storage, and other services. In that context, our partners are the controllers, and because we handle some personal data on their behalf, e.g., by storing it in our data centers, we are a processor. How GDPR regulations affect you depends greatly on this role definition.

3

Get a handle on the GDPR compliance posture of any sub-processors and third-party contractors you use that touch your customers' personal data. For example, if you use providers of application hosting, web hosting, SaaS, cloud storage, or other services, they are probably storing some personal data of EU citizens on your behalf, serving as processors in GDPR terms, and so will need to be GDPR-compliant, too.

You may need to renegotiate contracts and/or service-level agreements with some of them to ensure they are taking the necessary compliance steps for processors. In the event they cannot meet your terms, you will have to find new processors who can in order to protect your own compliance posture. In the meantime, take a default stance of assuming responsibility for GDPR compliance issues on behalf of any processors you use, as you may be held responsible for them by your local supervisory authority.

For example, Acronis serves as a data processor to many of its partners. Those partners must obtain data processing amendments to their Acronis contracts that reflect how Acronis will support its partners in their capacity as data controllers under GDPR. Acronis plans to prepare an amendment that works for all of its partners and to automate the system of executing the amendments. These new contracts will be made available to our partners on Acronis.com. and in our Partner Portal far in advance of GDPR's 25 May 2018 effective date. Acronis will send notice to all of the partners in advance of the website go-live date, and again when the website does go live.

4

Take a detailed inventory of all customer, partner and employee data that you capture or handle as a controller and/ or processor to identify whether it falls under GDPR scrutiny. The definition of what constitutes personal data is much broader under GDPR than it was under its predecessor, the EU Data Protection Directive.

Personal data now includes any information that can be used to identify an individual, including IP addresses, cookies, mobile devices IDs, various types of location data, and biometric data like fingerprints and facial scans. Understand that you will have to ask data subjects for their consent or define a legitimate purpose for collecting personal data in each specific case.

GDPR also requires a lot of additional documentation and record-keeping on your part, including what you are doing to personal data, why you are doing it, to whom you may be disclosing it, where you are sending it, how long you are keeping it around, and how you are protecting it against damage and theft.

On top of that, you will need to document who your third-party processors are and how they answer this same set of questions. If that seems like a lot of work, it is. Taking an inventory of the personal data under your control or processing is an essential first step.

5

Analyze all of your data flows to understand where and when you are transmitting personal data to other countries or handing off personal data to third-party processors. GDPR pays a lot of attention to the physical location of personal data, and places fairly strict limits on where you can send, process and store it. As a rule, personal data should be stored within the EU or in the handful of countries the EU has approved as having "adequate" security. Other acceptable destinations include those governed by certain agreements that have been approved by a GDPR supervisory authority in advance: so-called Binding Corporate Rules, codes of conduct, and certification schemes.

Some countries that are signatories to international privacy agreements with the EU, such as EU-U.S. Privacy Shield Framework, are acceptable. Finally, certain "specific derogations" (exceptions to the rules) apply, as when your data subject consents explicitly to a destination with an understanding of the accompanying risks, or in the case of certain controller or processor contractual obligations or legal claims.

6

Assess how well you can honor your EU-based customers' rights to get copies of, make corrections to, and delete their personal data on request. This is an important new protection for citizens under GDPR. Honoring deletion requests, the so-called "right to be forgotten", is especially important, and will likely require new investments in technology, policies and procedures.

7

Use encryption as an essential means to protect personal data against security breaches. Where possible, encrypt personal data wherever it resides in or traverses your organization: in transit over local- and wide-area networks, and at rest in your own data storage and backup infrastructure and services, or those of any third-party processor you use. An incident in which a hacker steals strongly-encrypted personal data without a decryption key is still considered a confidentiality breach, but may not lead to personal data disclosure, and so may not require that you report it to the supervisory authority or your customers.

8

Move to more granular monitoring of your IT environment. GDPR requires organizations to implement "adequate" security controls. If your systems have event logging, dashboards, and other real-time monitoring tools, enable them and make sure a staffer routinely reviews them. These will improve your responsiveness to potential security breaches and other ways of losing personal data (like hardware failures and IT staff errors). They will also be helpful in the event you need to demonstrate to your supervisory authority that you took appropriate measures to defend against losses of personal data, that any breach was not the result of your own error or malice, and other potentially exonerating circumstances that could save you from a large fine.

9

Review your policies regarding recovery from security incidents, particularly your procedures for notification of supervisory authorities, business partners, and customers in the wake of a serious breach. GDPR requires you to act within 72 hours of discovery of a breach, and in some cases to notify all affected data subjects without undue delay.

10

Conduct a security risk assessment to identify your most serious potential sources of breaches. For example, certain industries like healthcare, government and financial services have come under increasing attack by ransomware, the fastest-growing malware threat of recent years. Focus on improving your defenses on the highest-probability threats. It is far simpler and less costly to stop a malware threat before it occurs than to undergo the post-breach mitigation and reporting protocols required by GDPR.

11

Drill, test, and audit your data protection and IT security environment and staff. Run data breach simulations on a regular basis to see how well your staff knows its roles and responsibilities under GDPR. Practicing your response to a data breach ahead of time can save you significant non-compliance penalties when it happens for real.

12

Get qualified legal advice. Perform a legal review of your GDPR compliance status. All of your IT vendors are certain that the answer to your GDPR problem is what they're selling. Don't rely exclusively on them.

Note: *This checklist is for informational purposes only. This checklist is not intended to and should not be relied upon or construed as legal advice. You should not act or refrain from acting on the basis of any content in this checklist without seeking legal or other professional advice.*

For additional information, please visit **www.acronis.com**

Acronis