WHITE PAPER

GDPR COMPLIANCE

A STEP-BY-STEP GUIDE TO AVOIDING STEEP FINES AND REPUTATION DAMAGE IN THE EUROPEAN UNION

CYBERSCOUT®

1

BEFORE YOU CAN BEGIN YOUR COMPLIANCE EFFORTS IN EARNEST, YOU WILL NEED A SUBSTANTIAL AMOUNT OF INFRASTRUCTURE, INCLUDING A DATA-TRANSFER MECHANISM, A DATA PROTECTION OFFICER, A CROSS-FUNCTIONAL TEAM AND THE ABILITY TO OPERATIONALIZE A REGULATION INTO THE WORKINGS OF YOUR ORGANIZATION.

INTRODUCTION

If your organization has a presence in the European Union (EU), it's probably subject to General Data Protection Regulation (GDPR). If that's true, and you're non-compliant on May 25, 2018, your organization could incur fines up to 20 million euros or 4 percent of its total worldwide annual revenue—whichever is higher.

With more time, you could develop an overall business strategy around the GDPR and connect your compliance efforts with your business goals, mission, vision and values. You could demonstrate the aligning of key business objectives and measure performance with performance indicators and perhaps even run pilots in different departments.

It's too late for that now.

Read this guide to immediately to learn where to begin and how to proceed. Don't take any chances.

We've studied the GDPR since its launch, and helped dozens of clients plan for compliance. Today, we've identified the essential tasks GDPR-subject companies must have implemented before next May:

1. Solidify your data-transfer mechanism
2. Tap into your team's collective intelligence
3. Map out your company's data ecosystem
4. Identify and prioritize gaps in your compliance posture
5. Plan your path to compliance
6. Return to business strategic planning.

Start now. Contact us if anything is unclear or seems unattainable.

To your successful compliance,
CyberScout® Solutions

2

EACH MEMBER OF YOUR CROSS-FUNCTIONAL TEAM WILL REPRESENT A DEPARTMENT AFFECTED BY THE GDPR. THEIR COMPLEMENTARY INPUT WILL BE INVALUABLE FOR ENSURING YOUR COMPANY'S COMPLIANCE.

Three terms you need to know

- **Data subject** – A natural person in the EU whose personal data is processed by a controller or processor. They're your users, customers and employees.
- **Personal Data** – For the purposes of this handbook, let's confine 'data' to mean information protected by the GDPR that can be used to identify an individual directly or indirectly, such as a name, a photo of the data subject, an email address, bank details, etc.
- **Processing** – Any operation performed on personal data, such as collecting, organizing, storing, altering, using and disclosing.

SOLIDIFY YOUR DATA-TRANSFER MECHANISM

If your company operates in the EU but handles data elsewhere, you'll be transferring data across the economic region's borders. Whether you choose to self-certify according to the EU-US Privacy Shield pact, a model clause agreement, or another mechanism, international law holds you accountable for providing adequate safeguards, such as protecting the confidentiality, integrity, availability and durability of the data you're transferring.

For those of you still declaring your organization's compliance with the US-EU Safe Harbor Framework on your website as the legal mechanism to legally transfer data from the EU to the US, Safe Harbor died in October of 2015. Unless your organization relies on another data transfer mechanism, you have been transferring and continue to transfer data illegally.

While you're planning and implementing the rest of the suggestions in this guide, certify immediately to participate in the data-transfer mechanism that best suits your organization.

HIRE A DATA PROTECTION OFFICER (DPO)

This individual will lead your organization's efforts to comply with the GDPR. Your company may be required to have a DPO if it:

- Monitors data subjects on a large scale
- Processes special categories of data (e.g. racial, ethnic origin, political, health, etc.) on a large scale.

The GDPR doesn't specify the exact credentials DPOs must carry, other than requiring "expert knowledge of data protection law and practices." The level of

3

CREATE A QUICK REFERENCE THAT WILL HELP ALL MEMBERS OF YOUR TEAM AND THEIR RESPECTIVE DEPARTMENTS TO UNDERSTAND HOW THE GDPR APPLIES TO THEIR WORK.

that expert knowledge will be influenced by the protections required for those data you process.

DPOs may do other work in your company as long as there is no conflict of interest.

Even if your organization isn't required to have a DPO, you still need someone to manage your compliance effort. Hiring, assigning or outsourcing such a role should be a top priority. Their familiarity with the discipline of privacy will be invaluable.

ASSEMBLE A CROSS-FUNCTIONAL GDPR TEAM

Because data are so important to so many different parts of a company's operations, the GDPR's mandate will impact most departments.

As such, the DPO should assemble a team of people who represent each of the affected business departments. At a minimum, we recommend the team include:

Leadership

The more leadership involved in the team, the better. Because they control budget dollars, they must understand the business risks and fines for noncompliance. Without leadership calling for compliance as a priority, the whole effort risks falling to the back burner.

Information Security

The GDPR mandates a variety of protective measures and best practices for the confidentiality, integrity and availability of the data you handle. The regulation includes resilience, too. You must be able to restore availability in cases of loss.

Your security team must become familiar with the GDPR's articles on information security and confirm that their data protection tools and procedures are adequate.

If your organization doesn't have a dedicated information security team, then involve the person on your IT team who is responsible for security.

Privacy

If your organization has a chief privacy officer, their organization-wide knowledge of privacy practices will make a superb addition to your GDPR compliance team.

4

ESTABLISH POTENTIAL RISK AREAS AND FOCUS ON WHERE YOU NEED TO COME INTO COMPLIANCE MOST. GET EXPERT GUIDANCE IF YOU NEED IT.

A privacy representative will raise questions centered around the spirit of the GDPR, such as: “Why do we need this data?” “Are we using it solely in the way that we said we would?” And, “Did we give adequate choice to consent?”

Compliance

Compliance professionals bring internal knowledge about how operations work in compliance. To play their essential part on the GDPR compliance team they need a thorough overview of the regulation and its application to your organization.

In the future, your organization’s GDPR compliance will need to be audited. If that work falls to someone in compliance, it will be expedited by their participation on your GDPR team.

Legal

Legal counsel will serve two roles in your GDPR compliance efforts: interpretation and documentation.

The regulation clearly states the characteristics of subject organizations. It’s up to your organization to decide whether and to what extent it’s subject. Turn to your legal counsel for a formal opinion. Then, document that opinion in case it’s called into question in the future.

For that matter, your legal counsel should document all of the team’s decisions; from collection to processing to storage of data.

Then, if the DPO or supervisory authority raises an issue, you can reference that documentation to defend the reasoning behind your decisions.

Marketing

In many organizations, this group gathers data from more sources than any other. With the team’s help, they’ll answer many of the questions at the core of the GDPR. See the section about creating a data-activities map for more detail.

Human Resources

In tandem with marketing, HR may be the one of the best groups to answer the questions in the data-activities map. Their knowledge will be instrumental in creating a defensible reason for collecting, processing and storing data about EU citizens who work for your organization.

Operations

Operations has a more granular view of your organization, including third-party services that may qualify as processors under the GDPR. In that case, the service—perhaps a SaaS platform—may accidentally gain access to protected data while providing technical support. It’s up to operations to know the extent of that exposure and its impact on your compliance posture.

5

YOUR ORGANIZATION WILL NEED TO MAKE CHANGES TO THE WAY THAT IT HANDLES PERSONAL DATA. BEYOND COMPLIANCE, THE BENEFIT OF TAKING ACTION NOW MAY MEAN LOWERING YOUR

Board member

The board must be kept informed of the entire effort: why your organization is subject to the GDPR, why this compliance effort is urgent, and the progress toward compliance. Because of the potential impact of the GDPR's fines, the board should get an update about compliance every time it meets.

CREATE A DATA-ACTIVITIES MAP

A large part of your cross-functional team's work will revolve around mapping out how your organization uses protected data. The map can take whatever shape that best suits your organization.

Larger organizations that use software to map their IT networks may be able to render a representation as a useable map. This is more suitable for entities whose data processes change regularly and must conduct Privacy Impact Assessments regularly (described in "Plan your path to compliance"). Software may help alert the Data Protection Officer to changes that require a PIA.

Smaller companies may find that a simple spreadsheet will suffice.

You'll want to map out answers to these questions:

1. Why are we collecting these data?
2. Where are we collecting them?
3. What is the basis for processing these data?
   - Do we have the data subject's consent on file?
   - Did the data subject ask us to keep these data?
   - Is our action in the public interest or for public security?
   - What "legitimate interests" (by the GDPR's definitions) are we pursuing?
4. What are we doing with these data?
5. How are we transferring them (across the organization and across political borders)?
6. Where are they stored?
7. How are they accessed?
8. How long are we keeping them?

The data activities map is a living document. It will change. We recommend auditing it every six to 12 months and updating it with each PIA.

6

IDENTIFY AND PRIORITIZE GAPS IN YOUR COMPLIANCE POSTURE

Now that you know how your organization uses data, assess how well your current operations comply with the GDPR.

Develop an assessment based on the GDPR's articles. They represent a natural starting point. Note that some articles contain multiple potential action items.

You might run out of time before reaching full compliance. We recommend you begin by addressing the following high-risk, high-fine items first.

1. Data subjects' rights

The GDPR protects European Union citizens' right to privacy as a fundamental human right. If you don't have a program handling data rights, begin that process before you finish creating your data-activity map.

2. Consent

The most common lawful basis for collecting data. Data subjects must understand what they're consenting to, and make a physical affirmation that they're actually giving consent. It will no longer suffice to present pre-ticked boxes on sign-up pages.

What's more, the data subject must be able to withdraw their consent at any time.

3. Legal data-transfer mechanism

As mentioned earlier, this is a prerequisite to comply with the GDPR.

4. Organization-wide principles

Expect to hear the phrase "privacy by design" and "privacy by default" more and more. These two principles are intended to promote the consideration of privacy as a fundamental component of an organization's operations. In practice, "privacy by default" would mean a new user's account would be preset with the strictest privacy settings. Privacy by design would make privacy a priority across your organization.

8

PLAN YOUR PATH TO COMPLIANCE

Master the Privacy Impact Assessment

Any time you make a change that affects the way you handle personal data, you must conduct a PIA. First, determine whether the change affects personal data. If it does, then you must update your data activities map and make changes to protect those data. If the change won't affect personal data, document the reasoning that led to that decision, and move forward.

Update policies, principles and procedures

Based on your gap analysis, you may find it beneficial to update the guiding vision of your organization. That change could cause a cascade of decisions and actions that will protect personal data and keep your organization compliant.

Choose tools that will aid compliance

Many of the third-party tools that you use to help you with your GDPR compliance may be exposed to those data you're obliged to protect. For that reason, your contracts with those vendors need to include a commitment that they'll comply with their obligations as processors.

Accelerate data-breach notification practices

The GDPR requires that you give notice of data breaches within 72 hours. Are your policies, procedures, and methods for monitoring data and networks up to the task?

Data minimization

Since the arrival of big data, companies have collected as much personal data as possible.

Now, your organization is responsible if it loses consumer data, including those data that it never monetizes.

That's why the GDPR requires subject companies to have a defensible reason for collecting, storing and processing personal data. If there is no reason, and local laws make no requirement to do so, then the data must be erased.

CONCLUSION

We believe that consumers around the world yearn for the level of data protection defined by the GDPR.

If you find it burdensome to maintain two different standards of data protection in your organization - one for GDPR-subject data, one for everything else - consider updating your entire organization's standards to

comply with the GDPR.

This practice may be the new minimum for the European market, but consumers in your other markets around the world may find your efforts so appealing that they choose to reward you with their loyalty and even advocacy.

Let us know how we can help.