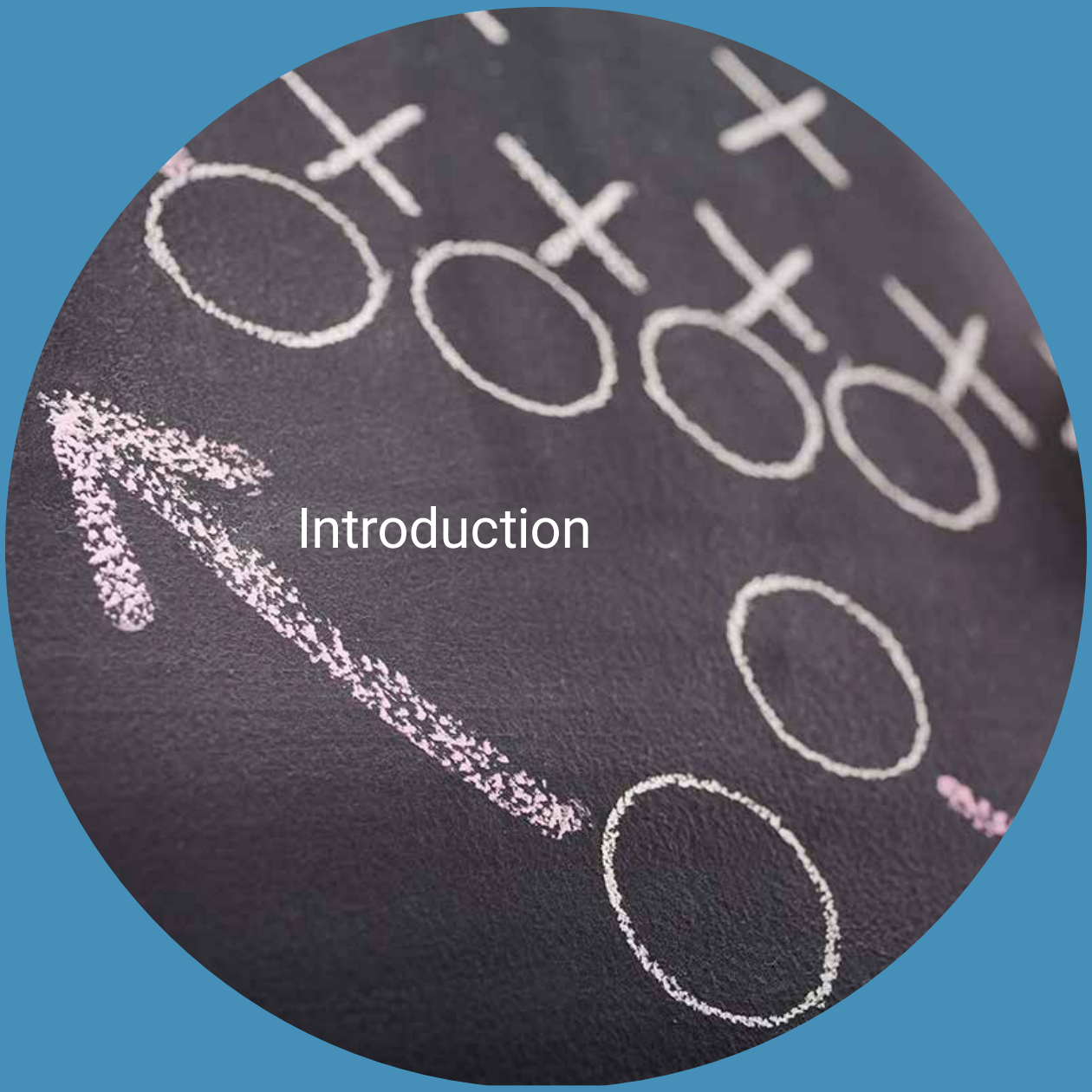
GDPR Playbook

Your Go-to Guide for Seamless GDPR Execution


Introduction

Introduction

The European Union's General Data Protection Regulation (GDPR) presents your business with an **opportunity**. By taking a proactive approach to its data handling and risk management requirements – by viewing it as a source of insight and competitive advantage, rather than an inconvenience – it can become a tool for business improvement.

It'll assist you in developing the plays that will help your organization beat the competition.

We recommend, at a high level, a simple, eight-step approach to ensure your organization is ready to comply with the GDPR.

If you successfully navigate these processes, you will have set up your business to reap numerous advantages, and avoid costly drawbacks:

8 Steps

1. Assign Responsibilities
2. Identify Personal Data
3. Describe Processing Activities
4. Implement Data Protection Impact Assessments (DPIAS)
5. Data Mapping
6. Technical And Operational Measures
7. Breach Management
8. Subject Right Requests

ADVANTAGES

Advantages include the efficiencies that arise from having compliant systems, improved brand reputation (to drive new business), competitive advantage over non- or less-compliant rivals, etc.

DRAWBACKS

Drawbacks include avoiding data breaches and the associated harms (fines, loss of consumer trust/brand reputation, and other penalties).


Assign Responsibilities

Assign Responsibilities

THE FIELD

GDPR **Article 4**, Definitions and **Article 5**, Principles relating to processing of personal data lay down the key roles and concepts governing the regulation. These include definitions of terms (e.g. personal data, processing, consent); and how data must be handled (e.g. is collected for specified, explicit and legitimate purposes, is processed in a manner that ensures appropriate security).

THE PLAY

Assign a team to audit your organization against Article 4 and identify your personnel and processes against them so you know where liability may arise (e.g. are you a controller, do you engage in cross-border processing, etc.). Audit against Article 5 and ensure you are compliant (e.g. that your data is processed lawfully, is accurate, etc.).

THE SCORE

By understanding how the GDPR's definitions and principles apply to your organization, you can effectively organize or modify activities to ensure compliance and begin reaping the benefits. These include advantages (such as customer trust, greater efficiency, and the advantages of operating with clean and trustworthy data), as well as avoidances (such as cost reduction, reducing liability and avoiding penalties).

Identify Personal Data

Identify Personal Data

THE FIELD

GDPR **Article 38**, Position of the data protection officer, describes the appointment of the data protection officer (DPO). **Article 37**, Designation of the data protection officer, details under what circumstances a DPO must be appointed, while **Article 39**, Tasks of the data protection officer, explains the DPO's duties.

THE PLAY

Appoint a DPO if required. The DPO's key responsibility is to be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. A DPO can be an existing or a new employee and might have other responsibilities. Regardless, it's vital to give them the authority and independence to do their job and minimize or remove any potential conflicts with other duties.

THE SCORE

In addition to being a regulatory requirement, an effective and empowered DPO makes for more efficient operations and stronger compliance performance. This in turn makes it easier for your organization to enjoy advantages including cost and efficiency improvements, reduced liability and greater trust from customers and regulators.


Describe
Processing
Activities

Describe Processing Activities

THE FIELD

GDPR **Article 30**, Records of processing activities, describes the types of records controllers need to keep about the processing activities they undertake, or which other processors undertake on their behalf. These include: names and contact details of relevant parties; details about the data's movements (e.g. to international organizations); when the data is likely to be erased; and more.

THE PLAY

Map your data flows so you have a clear view of how information moves to, from and within your organization. Put in place the data-gathering tools and processes needed to create a processing activity register – a "golden record" of the information required by Article 30 (broadly, a record of processing activities under your responsibility). This allows you to evaluate existing processes by using two simple filters: one to identify whether it's a business-critical process, and a second to identify whether you need further consent from affected data subjects. Audit your systems regularly and ensure your DPO has access to all relevant information.

THE SCORE

Your "golden record" makes it easy to determine whether your processing activities are secure and compliant. Documented proof of compliance is important if a breach occurs. More importantly, undertaking this review helps you identify potential weaknesses and security problems before they occur. It also makes breach detection faster and easier, which can help minimize the impact of many problems.

Implement DPIA

Implement DPIA

THE FIELD

GDPR **Article 35**, Data protection impact assessment, describes when a DPIA must be conducted and what information it must contain. Where new types of processing are being considered – and where personal data is being processed – the DPO must be brought in. The assessment must include: a description of the process or processes involved; risk assessments for the data subjects and processing operations involved; descriptions of risk management procedures; and more.

THE PLAY

Whenever new processes are being evaluated, the DPO should be involved in assessing *the impact of the envisaged processing operations on the protection of personal data*. If a DPIA is required, the DPO should supervise the assessment. You should also create processes and protocols to systematize DPIA creation. This will make conducting future DPIAs more efficient and ensure your approach is rigorous. Similarly, when a processor introduces or proposes a new service or data process, you need to have access to their DPIA.

THE SCORE

A DPIA is an important liability shield. Your DPIA will help ensure your processes fully comply with Article 35, while having visibility of your partners' will protect you against third-party liability. More importantly, it can identify problems in new systems before they arise, so they can be redesigned for security and compliance.


Data
Mapping

Data Mapping

THE FIELD

GDPR **Article 30**, Records of processing activities, describes the data-related records your organization must hold. More importantly, it mandates creating a record of processing activities that shows how data enters, moves through and exits your organization, and details other records to be kept.

THE PLAY

Create detailed maps of your data flows. These will help you understand your data-handling processes better, and also highlight any potential non-compliances, points of vulnerability, bottlenecks or inefficiencies. With this information you can remediate where necessary and ensure your data is secure and compliant. Think of these maps as your data "game plan."

THE SCORE

A good plan leads to a good score – using your data maps means you'll be prepared for whatever challenges come your way, with a good sense of how they'll impact your system and thus how to mitigate. The benefits of this can be considerable; if an incident occurs, compliance and good-faith efforts at mitigation can be considered when determining penalties.

Technical & Operational Measures

Technical & Operational Measures

THE FIELD

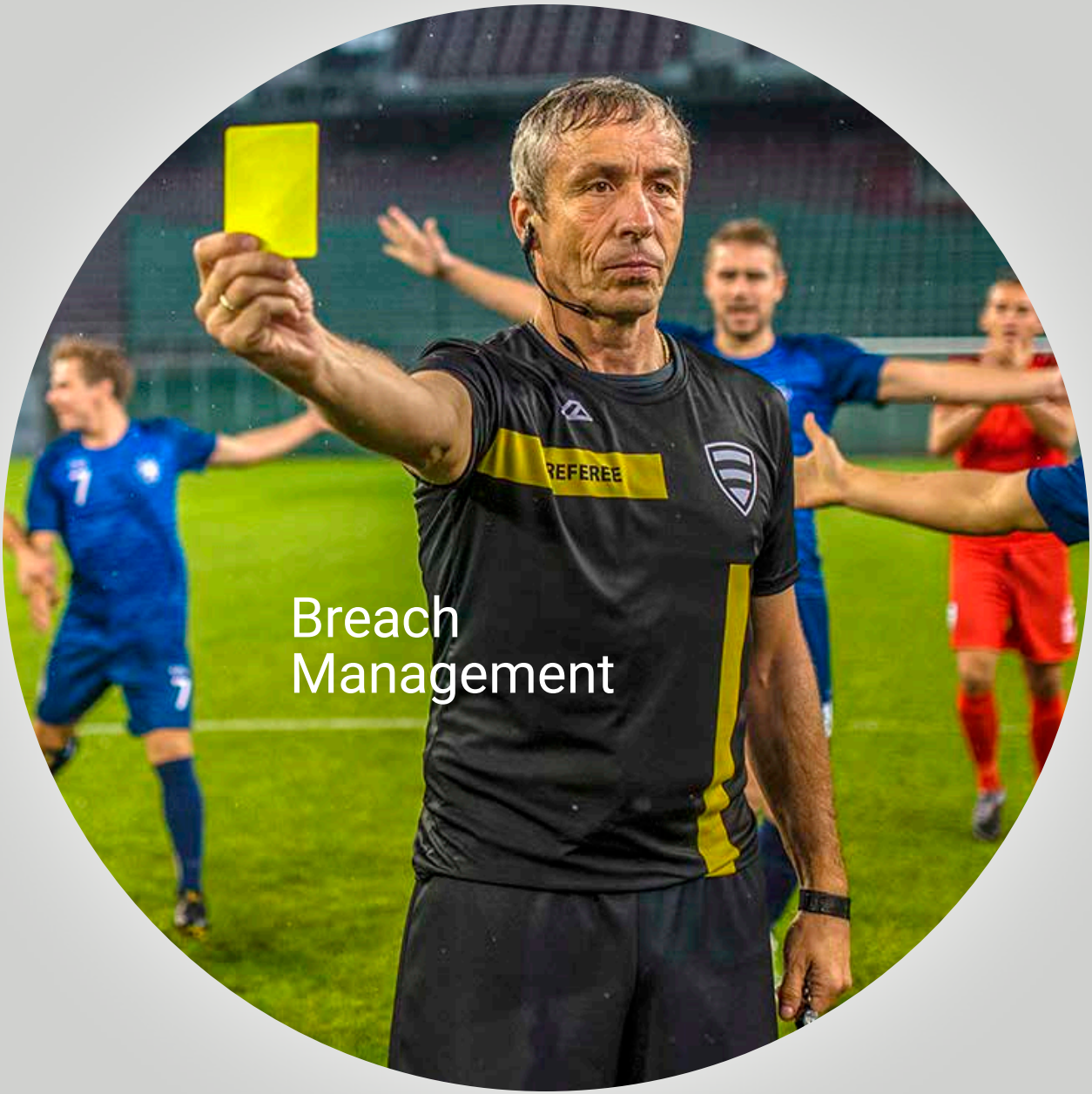
GDPR **Article 32**, Security of processing, describes how controllers and processors must consider the risks, costs and scope of their activity to ensure a level of security appropriate to the risk as assessed. Relevant factors include: the integrity of processing systems; the ability to restore access after an incident; and processes for ongoing evaluation.

THE PLAY

The DPO should be closely involved in assessing the measures to be implemented. Conduct regular audits to ensure your regime is appropriate and effective, especially if any part of your process, or the data you handle, changes. Implementing a code of conduct (**Article 40**) or approved certification mechanism (**Article 42**) can be used to demonstrate compliance. Finally, creating (or gaining access to) a comprehensive knowledge base will provide information on how to protect against various information security risks.

THE SCORE

This play can provide you with an easy win: secure systems are a key provider of major business advantages including greater efficiency, reduced costs, reduced likelihood of breaches and faster, more effective responses to any that occur.



Breach Management

Breach Management

THE FIELD

GDPR **Article 33**, Notification of a personal data breach to the supervisory authority, and **Article 34**, Communication of a personal data breach to the data subject, explain that breaches must be notified to relevant authorities within 72 hours and to relevant persons without undue delay. In some circumstances there is no need to notify of a breach, for example if breached data was unreadable or otherwise unusable.

THE PLAY

Put in place automated systems to detect breaches immediately and notify the DPO. Implement escalation and notification processes to ensure compliance with responsibilities. Commit to testing them on an ongoing basis to ensure their integrity and effectiveness.

THE SCORE

Fast action in the event of a breach can contribute to mitigation, prevent further losses and even assist in apprehending bad actors. It can also help maintain your reputation and public trust if a breach is notified to those affected. Understanding when to notify or not can similarly prevent bad news from becoming public.

Subject Right Requests

Subject Right Requests

THE FIELD

GDPR **Article 15**, Right of access by the data subject, **Article 16**, Right to rectification, **Article 17**, Right to erasure, **Article 18**, Right to restriction of processing, **Article 19**, Notification obligation regarding rectification or erasure of personal data or restriction of processing and **Article 20**, Right to data portability explain the various rights individuals have in regard to their data. All must be respected and complied with.

THE PLAY

Systems may need to be modified or adopted to enable compliance with any requests generated under these Articles. The costs involved may be significant, but they should not be avoided; the DPO will be closely involved and should ensure that data is accessible, and that requests can be evaluated and actioned (if deemed valid) promptly.

THE SCORE

It's not just a matter of bare compliance with the Articles; compliance can also bring important business benefits. For example, having transparent systems in place increases trust from customers and regulators, and prompt compliance can boost your reputation with affected and interested parties.

Conclusion

Successfully transitioning into the post-GDPR world doesn't need to be difficult. While there will initially be some short- and mid-term effort and expense involved to ensure compliance, we believe that in the mid- to long-term, the benefits far outweigh the costs.

The drawbacks – penalties and harms avoided – are reason enough to comply. But when you consider the advantages – that is, efficiencies gained – then it becomes a clear-cut decision. Compliance with the GDPR can transform your business, position you to gain rich insight into your processes, generate actionable business intelligence, and gain competitive advantage in the marketplace.

ALL YOU NEED DO IS TO MAKE THE RIGHT PLAYS.

SAI GLOBAL