gma© Global Marketing Alliance
INSIGHT FOR DATA DRIVEN MARKETERS

Data Protection Network

OneTrust
Privacy Management Software

Data Impact 2019:
Data Governance

Foreword

We are living through a transformative time in privacy. Personal data, big data analytics and artificial technology are being used to solve everything from small daily inconveniences to tackling the world's biggest problems. At the same time, consumers are aware more than ever about the human impact of abuse or over-use of their personal data.

Adhering to data privacy regulations like the GDPR is no longer just a checklist compliance item, but instead a moment where businesses can be transparent about data collection and build customer trust that they will use and process data in a responsible manner. The GDPR was a moment in time where the world collectively had a conversation about privacy, and today we are seeing the results of this dialogue.

Countries and regions across the globe are proposing and passing similar data privacy legislation, while companies are continuing to innovate and users are still consenting to the responsible use of their data.

OneTrust is proud to sponsor the Global Marketing Alliance and the Data Protection Network on the Data Impact 2019 report highlighting the importance of a sound data strategy. As the world's leader in privacy, security and third-party risk software, OneTrust provides the technology for companies to deliver transparency and trust to their consumers as well as reporting to regulators with the GDPR and other global privacy laws.

Together with partners like the Data Protection Network and the Global Marketing Alliance as well as our base of 2,500 customers, we are enabling business innovation and consumer trust in this transformative time in privacy, delivering solutions to help solve the world's problems, both big and small, with the fair and responsible collection and use of personal data. To learn more about how OneTrust can help operationalise privacy, security and third-party risk programs, visit **onetrust.com.**

Ian Evans Managing Director, EMEA OneTrust

Data Governance

OneTrust
Privacy Management Software

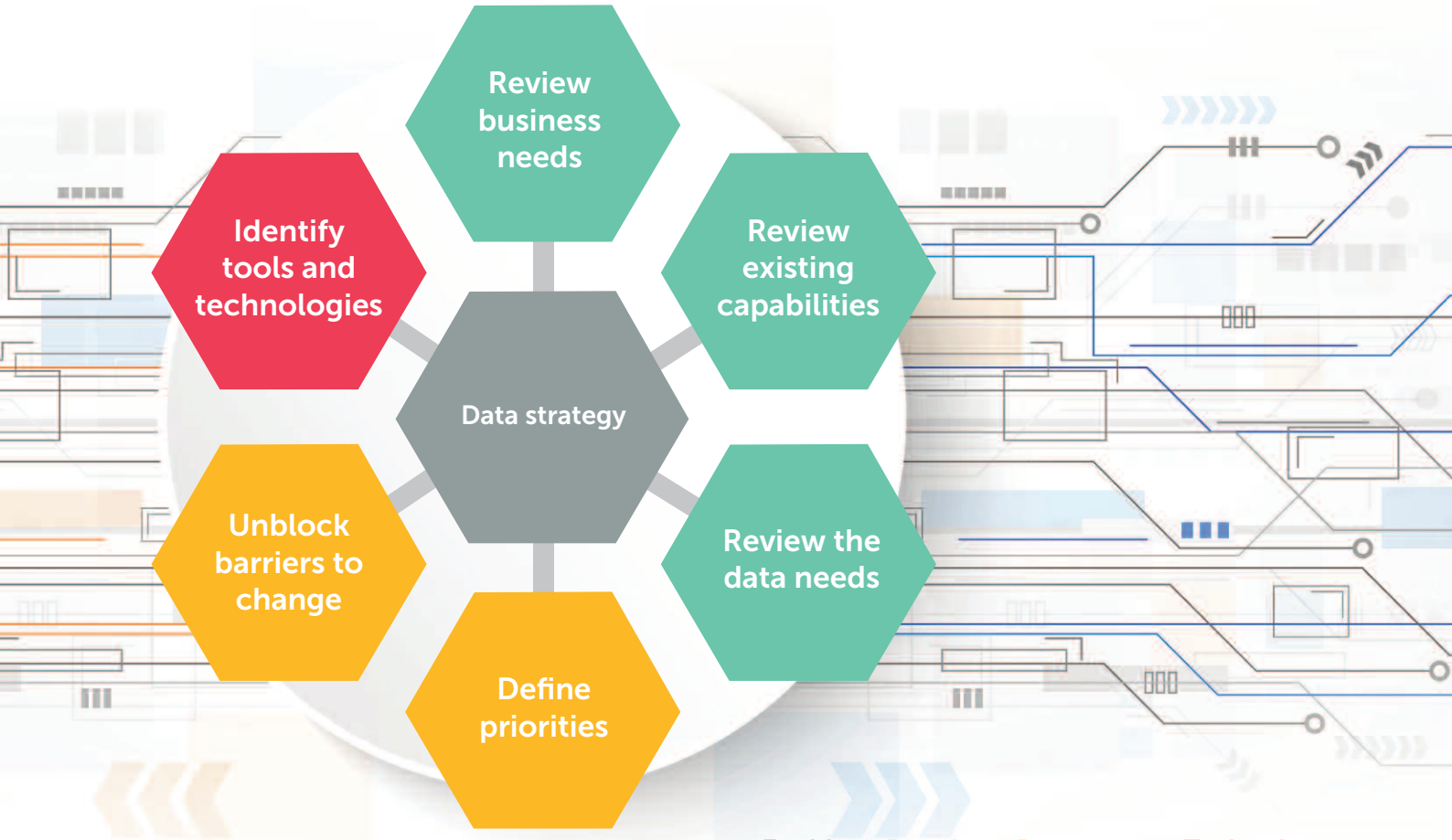
Why GDPR and Data Governance go hand in hand
Data governance is increasingly recognised as an important method of protecting businesses from legal, financial and reputational risks which can arise when processing personal data. In essence, investing the time and resources to create a robust data governance programme ensures the right foundations are in place to empower the business to make the most of its personal data assets in a safe and secure way. GDPR requires organisations to have in place disciplined, transparent and accountable procedures for processing personal data.

Personal data is often one of the most valuable assets of a business. To make it work profitably, you need to understand how you're using it and take responsibility for it.

Many organisations are striving to embed Privacy by Design and by Default across their data processing functions, to ensure compliant solutions are 'baked in'.

What is data governance?
Data governance is a holistic approach to data privacy and security. It is essentially a set of management practices which ensure that personal data is used and protected, according to law and best practices. It is a process by which you:

- Understand and protect the data assets of the business and the interests of your customers, employees and the public
- Ensure compliance with data & privacy laws
- Identify existing & emerging data risks so they may be properly assessed and mitigated (where necessary)
- Support data strategy & innovation



Enablers: People > Processes > Technology

Data Governance

An effective data governance framework can ensure that business objectives which utilise data can be met without taking unnecessary compliance risks.

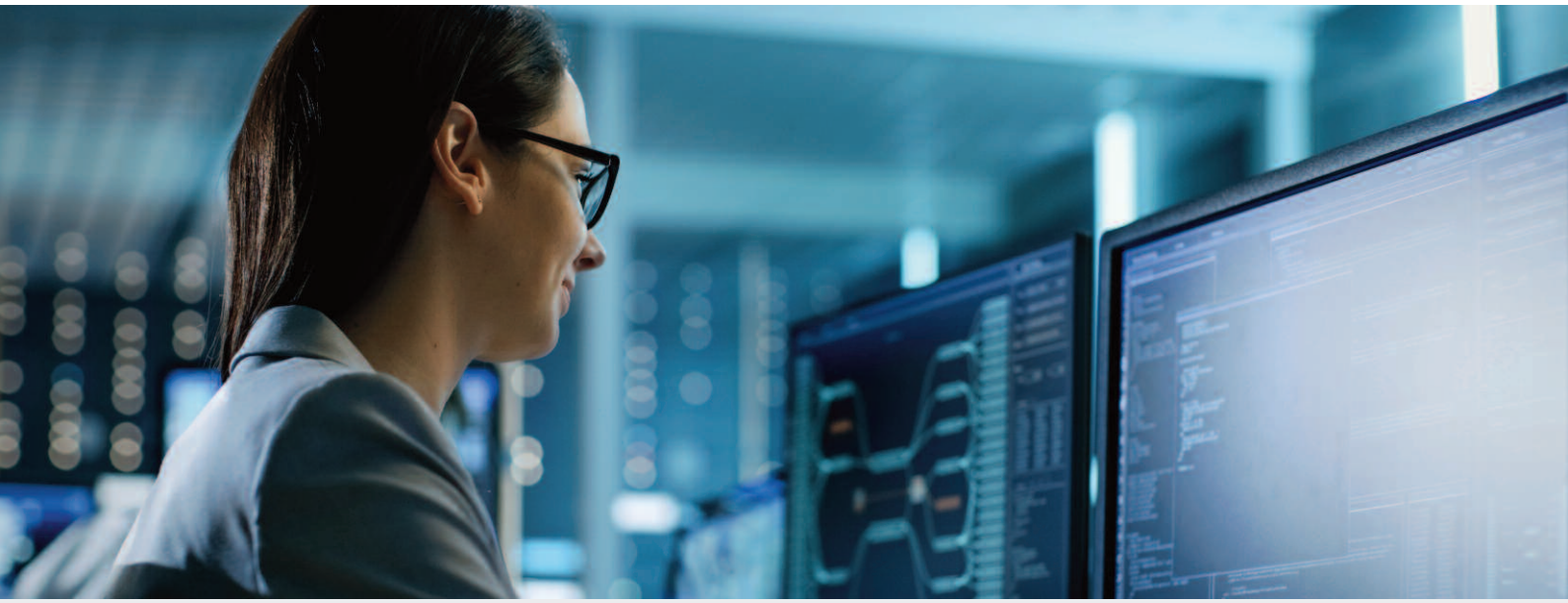
The challenges organisations face

- Many organisations don't have a recognisable data governance framework in place
- Distributed processing by many functions
- Outsourcing to third party processors - makes it hard to identify ALL of the processing
- Wider definition of personal data: more processing falls under scope of DP laws
- Lots of processing may never have been assessed before to ensure its fair, lawful, transparent and secure
- Legacy systems may not meet Privacy by Design standards
- Handling information rights - such as subject access and erasure requests
- Inexperience in carrying out data protection impact assessments

Get to know your data and how it is processed
Many different departments process personal data. Information that can relate to customers, staff, business clients, contractors/agents and other parties.

The first step is to assess the personal data being processed by the various business functions.

Above: Examples of some of the business functions which may process personal data



Data Governance

Assessing your data risks
Any data governance programme should include risk assessment processes to discover, assess, prioritise and take necessary action to mitigate compliance risks.

A data governance programme should provide tools to help your teams to identify both existing and emerging risks, so they can be properly assessed, and risks can be mitigated.

Data Governance

Data Protection Impact Assessments
GDPR sets out that in certain circumstances a data protection impact assessment (DPIA) is required. Notably when there is a significant change to existing processing, or new processing which may give rise to high risks for data subjects. As part of your governance framework you will need to ensure you and your teams are able to identify when a DPIA is required, or when you may decide it would be appropriate to conduct one voluntarily.

A DPIA should be carried out at an early stage when you are planning to implement new systems, technologies or processes. The aim is to identify any privacy or security concerns early on so that compliant solutions can be agreed during the early states.

Consider a DPIA as acting like an early warning system of emerging risks, alerting the business before those risks become reality. A documented assessment also provides valuable evidence of your compliance endeavours.

Does your organisation need a DPO?
The GDPR introduces a duty for organisations to appoint a data protection officer (DPO) if they are a public authority or body, or if they carry out certain types of processing activities. DPOs assist an organisation to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding DPIAs and act as a contact point for data subjects and the supervisory authority (e.g. the ICO).

Some organisations fall under the mandatory requirement to appoint a DPO, others have chosen to voluntarily appoint one. Even if you don't consider you need a DPO, you should appoint someone or a group of people who are responsible for data protection and governance within your organisation.

Role of the DPO

- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level
- A DPO can be an existing employee or externally appointed
- In some cases, several organisations can appoint a single DPO between them.
- DPOs can help demonstrate compliance and are part of enhanced focus on accountability.

Train your people how to protect personal data
A core component of a data governance programme is ensuring your employees are provided with high quality data protection training. Your people don't just need to know how to handle your data appropriately and to ensure individuals' rights aren't undermined, but also crucially need to know how to prevent a personal data breach.

Debbie McElhill, Associate at data protection consultancy Opt-4 stresses the growing need to take data governance more seriously:

"Make data governance a key priority. Get it on the boardroom agenda as part of the customer strategy and keep educating your people. Be creative in how you do that. If your business is unfortunate enough to become the subject of an ICO investigation, then you can bet they will ask you how you trained your staff and will want to see evidence of that training. Having a sound data governance framework requires you to fully train everyone in the organisation who processes personal data. Looking after individuals' personal data compliantly needs to be embedded as part of your company culture, it needs to be second nature for your people - just like great customer service should be."

Data Governance

Be proactive and diligent
The job of compliance is never done, so the need to keep abreast of legislative changes and update training and processes where appropriate will continue.

Those who wish to create a customer focused culture, which places the needs of consumers and individuals first, will want to protect their customer data from harm and therefore will be better able to adjust to legislative changes as and when they occur.

Outsourcing to data processors
Third parties could be the weakest link in a company's data security. Outsourced processors were implicated in more than 60% of all data breaches pre-GDPR and some of the largest financial penalties for data control failures were a consequence of third-party actions.

Due diligence of third-party providers is now key, as Ian Evans, VP at global data protection specialists, OneTrust, explains:

"You now have the obligation to ensure that the people you contract with - and who undertake processing on your behalf - are also going to represent you and your views on privacy as well."

Winning hearts and minds
The more your customers trust you, the more they will be prepared to share their personal information with you. Demonstrating that you take privacy seriously will also benefit your business relationships. People are more aware of their privacy rights than ever before and organisations are increasingly wary of doing business with companies lacking sound privacy credentials.

Simon Blanchard, Chair of the Data Protection Network and Senior Associate at Opt-4 says:

"Data protection and privacy professionals face a cultural challenge to win hearts and minds. I have sometimes heard Legal or Privacy teams described as 'The department of no' - seen as putting obstacles in the way of innovative ideas and strategies with data. That's not how we want to be seen. We should help our business colleagues to balance the needs of commercial and operational functions with the legal requirements. We need to go a step further than explaining the law – we must help them to find pragmatic solutions. Collaboration and mutual understanding are essential ingredients for successful data governance.

Forward-thinking organisations have recognised that good data governance & privacy credentials can really help to build customer trust and become a brand asset. Business objectives can be met without taking unnecessary compliance risks when we work together."

gma© Global Marketing Alliance
INSIGHT FOR DATA DRIVEN MARKETERS

www.the-gma.com

Follow us on Twitter @gmainsight

Join our Linkedin Group for data driven marketers

Data Protection Network

www.dpnetwork.org.uk

Follow us on Twitter @dpntweet

Join our Linkedin Group

OneTrust
Privacy Management Software

www.onetrust.com

Follow us on Twitter @OneTrust

Join our Linkedin Group