integreon

# Sound Governance for Personal Data

Tuesday | January 7, 2020
by **Clare Chalkley**, Vice President - Legal Services, Integreon
and **Claire Frazer**, Director - Legal Services, Integreon

## Data is on everyone's mind these days. Personal data, data security, data privacy, data breaches, data governance – all these terms dominate today's headlines and C-Suite discussions.

Data is often thought of as a mass of information, but data defines anything from a single piece of identifying information to a seemingly infinite supply of emails, documents, graphics, multimedia recordings and more.

Due to sheer volume and frequency of mention, data has become an abstract technical concept, but data itself is not abstract. Data has real effects on people's lives and on a company's reputation. Data is what proves identity and individuality, and as such it is not a collective thing. Each piece of data can be linked to a specific individual and organisations at fault for loss or reckless treatment of data can face severe penalties.

> **A driving principle behind GDPR is to provide individuals with more control over and access to their personal data stored by entities with which they interact.**

For purposes of privacy and security, organisations must have a clear understanding of the data they hold and be prepared to justify why they have it, how they use it and who they share it with.

In force since May 2018, the GDPR regulation safeguards EU citizens' rights to access and control their personal data. A driving principle behind GDPR is to provide individuals with more control over and access to their personal data stored by entities with which they interact. Under certain circumstances, GDPR can also award individuals the right to be forgotten and to have their personal data erased.

Personal data is defined as identifying information relating to a living person. That data can exist in many different formats across multiple systems such as:

- Hard copy / paper and electronic documents
- Human resources files
- Email systems
- Company laptops
- Server data
- Recordings of phone calls
- Closed-circuit television (CCTV) footage from security and other video cameras
- Messages sent via internal messaging systems, via SMS, WhatsApp
- Client databases
- Sales databases

GDPR is broadly focused, not only protecting numbers and names, but also protecting revelation of personal traits and preferences such as health records, religious and political affiliations, and sexual orientation.

Backed up by fines and penalties for violations, GDPR has motivated corporates to face their responsibilities as data controllers and/or processors. In this new culture of GDPR-driven accountability, companies doing business in the EU have had to establish policies and procedures around GDPR and ensure they are compliant.

Key to this compliance is strong data governance.

To establish a strong data governance policy, organisations need to understand the following:

- What data is collected and who does it belong to ?
- Why it was collected ?
- How and where it is stored ?
- Who has access to it ?
- How it is shared and used ?
- How long is it being retained and is it purged when retention is no longer required ?

Maintaining GDPR compliance requires an ongoing process of monitoring business practices. Data governance is crucial and data protection policies and controls need to be regularly assessed in order to remain up-to-date. Key documents such as internal staff privacy notices and public-facing privacy notices must be accurate. Continuing compliance activities may include conducting impact assessments for new

**DSAR is a term introduced in the GDPR legislation. A DSAR provides individuals with a mechanism to obtain copies of the personal data an organisation holds on them.**

systems, reassessing security procedures, providing GDPR training refreshers for existing employees, incorporating GDPR training into the onboarding process, and analysing new and existing contracts and agreements to ensure that data processing meets the requirements of GDPR.

DSAR (Data Subject Access Request) is a term introduced in the GDPR legislation. A DSAR provides individuals with a mechanism to obtain copies of the personal data an organisation holds on them. Since May 2018, DSARS have become widespread and very common. Individuals can "DSAR" an organisation (in writing or verbally) as many times as they like (within reason) and pay no fee. The organisation then has one calendar month to respond to the DSAR, with the day of the request's receipt counting as Day 1, regardless of the DSAR's scope. Some individuals intentionally "DSAR" a company repeatedly as an act of defiance or retaliation. As the circumstances in which an organisation can refuse to comply with a DSAR are very narrow, the pressure is on.

Responding to a DSAR can be a major business disruptor and a drain on multiple internal resources across an organisation. The response process often requires a collaborative effort from multiple teams including HR, IT and in-house counsel.

Larger companies may have designated Data Protection Officers whose primary job it is to deal with DSARs and other data privacy issues, and that can help alleviate the workload of others. However, the best defense against DSAR disruption is for companies to ensure they have a tried and tested DSAR response workflow, spanning from the moment the DSAR is received through to document production and fulfillment of the request.

**Cyber incidents can affect any organisation around the globe, not just those who are subject to GDPR compliance requirements.**

Having a robust data governance not only serves to satisfy GDPR requirements but also stands an organisation in good stead if a cyber-incident or data breach occurs. Cyber incidents can affect any organisation around the globe, not just those who are subject to GDPR compliance requirements. When a cyber-incident or breach occurs, organisations must quickly determine the extent of the data exposure and notify all individuals impacted by the breach.

In the US, insurance companies, law firms and cyber/computer forensics consultants have just 45 days to inform impacted individuals about the incident. In the UK, there is no definitive timeframe but if the breached data is high risk, organisations must notify individuals "without undue delay".

Fully responding within such tight timeframes is a challenge, given that each person whose data was impacted may have had a different combination of personal identification and health data exposed by the incident. With cyber incidents as with DSARs, the importance of tracking personal data on a one-by-one level is abundantly clear.

In summary, keeping data secure and clean is an ongoing commitment that organisations categorically cannot avoid. Data breaches will occur, DSARs will be issued and these may seem like an impossible, unfair burden for the organisations affected. However, with robust data governance, tried and tested procedures in place to identify and collect the potentially responsive data, and the right resources engaged to analyse and review the documents, the process can be streamlined and obligations can be fulfilled with minimum negative impact to the business. Engaging an experienced service provider like Integreon, who has worked on a large number of data breach and DSAR reviews both onshore and offshore over the past 2 years, will ensure that there is a consistency in approach and accuracy across the work product.

# About the Authors

**Clare Chalkley**
Vice President
Legal Services,
Integreon

Clare Chalkley is VP Legal Services at Integreon and is a subject matter expert for eDiscovery and Managed Document Review. She joined Integreon in April 2019 after serving as Litigation Support Manager for 25 years at Clifford Chance, a multinational law firm where she headed up the eDiscovery and Case Management team, supporting lawyers and clients around the global network on litigation and arbitration matters, regulatory, internal and anti-trust investigations and employment disputes. She is on the board of ACEDS UK Chapter (Association of eDiscovery Specialists) and is actively involved in the organisation and delivery of educational events.

**Claire Frazer** Director
Legal Services,
Integreon

Claire is the UK Director based at Integreon's London office. Claire is responsible for the operational management of our London Delivery Centre and oversees the delivery of all Managed Document Review and Cyber Incident Response services in the UK. Claire was admitted to practice law in England and Wales in 2008 and, before joining Integreon in early 2013, Claire was a practicing lawyer who gained extensive experience in a number of disciplines, including litigation. Prior to her current role of Director, Claire was engaged as a Senior Project Manager who managed an extensive variety of projects involving complex litigation, regulatory proceedings and government investigations, for a range of organisations, including Fortune 500 clients, large financial institutions and some of the world's top ranking law firms. Claire's experience spans a wide range of review workflows, from basic linear review to complex, analytics driven, workflow solutions.

# About Integreon

Integreon is a trusted, global provider of award-winning legal and business solutions to leading law firms, corporations and professional services firms. We apply a highly trained, experienced staff of 2,400 associates globally to a wide range of problems that require scale and expertise, enabling clients to become more operationally efficient by streamlining operations, maximising investment and improving the quality of work they provide their end clients. With delivery centers on three continents, Integreon offers multi-lingual, around-the-clock support, as well as onshore, offshore and onsite delivery of our award-winning services.

For more information about Integreon's extensive range of services

Email: **info@integreon.com**, Visit: **www.integreon.com**

and Follow: