GDPR Cheat Sheet

12 important takeaways from the looming General Data Protection Regulation

STAR COMPLIANCE

www.starcompliance.com

On May 25 the General Data Protection Regulation, or GDPR, goes into effect. Years in the making, it will fundamentally change how companies that interact with EU citizens do business. Why was it created? What's in it? How will it affect your enterprise financial institution? Here are 12 important takeaways.

01 What is it and why now?

The GDPR is a new set of data-privacy rules, which will supersede the current regime: 1995's Data Protection Directive, or DPD. The EU felt there had since been a fundamental shift in how individuals, companies, and governments interact when it comes to data, not just in volume but the ease with which it flows.

02 What types of businesses will the GDPR affect?

Any company that does business with EU citizens, or monitors their behavior, will have to comply, no matter where in the world it's based or where its work is done. If services are free, the GDPR still applies. And unlike the DPD, the GDPR will apply to data processors as well as data controllers.

03 What's at the heart of the GDPR?

The GDPR is all about the data privacy of the individual. Like the DPD, the GDPR focuses on the data privacy of the data subject. For the EU this concept is fundamental, and data privacy is essentially seen as a human right for EU citizens. A data subject is any person who is the subject of personal data.

04 Doesn't the DPD protect individual data rights?

Yes, but not with the same finality as the GDPR. As their names denote, the GDPR is a regulation and the DPD is a directive. The day the GDPR goes into effect, it becomes law across the EU.

05 Does consent change under the GDPR?

Yes. Requests for consent must be written in clear, intelligible language. No more legalese. People must know exactly what they're agreeing to. And it must be as easy to withdraw consent as it is to give it.

06 What other data-subject rights will there be?

- **Right To Breach Notification.** Data controllers must notify customers of any breach within 72 hours. Data processors must notify their data controllers immediately in the event of a breach.
- **Right To Access.** Data subjects have the right to know if their personal data is being processed, where it's being processed, and for what purpose.
- **Right To Data Portability.** Data subjects have the right to transmit their personal data to another controller, which must be provided for free in an easily accessible electronic format.
- **Right To Be Forgotten.** Also known as data erasure. Data controllers will be required to erase a data subject's personal data and cease further dissemination and processing if the data subject asks.

07 Will the GDPR affect data-system design?

Yes. Privacy By Design will be a legal requirement under the GDPR. It calls for data protection to be designed into collection and processing systems from the start, rather than as an afterthought.

08 Will we have to hire for any newly required positions?

Possibly. The GDPR creates a requirement for Data Protection Officers, or DPOs. DPOs will only be required for controllers and processors that monitor data subjects on a large scale. The DPO could be a new employee, an existing employee, or an external service provider, so long as he or she is qualified for the job.

09 How does Brexit fit into all this?

Brexit is still very much a work in progress, but if you'll be controlling or processing data on EU citizens on or after May 25 you'll need to comply with the GDPR. Period. No matter what form Brexit ultimately takes and no matter where in the world your company is based or does its work, including the UK.

10 Will exporting data out of the European Economic Area still be banned?

Yes. It was banned under the DPD and will remain banned under the GDPR, though there will be "adequacy" recognition for territories, sectors, and member states.

11 What if we don't comply with the GDPR?

Serious breaches can mean a fine of 4% of annual global turnover or €20 million. Less serious breaches can mean a 2% fine. Data Protection Authorities, or DPAs, will also have mandatory audit rights.

12 How does the GDPR affect Star and its clients?

Like any data processor, Star will need to convey where systems are located, report breaches, and appoint a DPO. It will also have to follow recognized security measures, erase data when it's no longer relevant, make Privacy Impact Assessments, and employ Privacy by Design.

The good news is, at Star we already do all of this, and easily meet all forthcoming GDPR requirements. We even have a new Data Retention, Archiving & Destruction module in the works.

If this quick-take was helpful and you'd like to learn more about the GDPR, read part one and part two of our blog series. In it, you'll find in-depth information on this expansive and historic piece of EU legislation.

Interested in learning more?

Are you ready to speak with a Star representative about your compliance platform needs? If so, email us at **info@starcompliance.com**.