By Christiana Kouppi, G. Vrikis & Associates LLC

GDPR

Ten GDPR Questions You Should Know the Answer to

Getting in touch with Christiana Kouppi, we talk about the much discussed topic: GDPR. With it being over a year since the regulation came into effect, Christiana answers the 10 most FAQ questions on GDPR.

"People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."
- *Information Commissioner Elizabeth Denham*

1. So what is GDPR?
GDPR stands for General Data Protection Regulation and it is Europe's framework for data protection laws, replacing the previous 1995 data protection directive.

The aim of the Regulation is to ease and safeguard the flow of personal data across the EU Member States. Being an EU Regulation, it is directly applicable to each Member State's national law.

GDPR legislation came into force across the European Union on 25 May 2018 and one of the main benefits of the GDPR is that companies are now required to demonstrate that they are actively working to protect their customer's personal data, and can be fined heavily if they become complacent about data security.

The GDPR outlines a range of rights that each individual in the EU has when it comes to their personal data:
1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

2. Who does the GDPR affect?
Essentially everyone. Almost every aspect of our lives revolves around data and almost every service we use involves the collection and analysis of our personal data. GDPR applies to any company or organisation operating within the EU, as well as any company or organisations outside of the EU offering goods or services to customers or businesses in the EU.

3. What do we mean by personal data?
GDPR applies to 'personal data', meaning any information relating to a recognisable person who can be directly or indirectly identified in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or even online identifiers, which include IP addresses. An example given is if you provide free WIFI in your building and collect the IP addresses of all users, this will be caught by the GDPR.

4. What does 'processing' mean?
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or the alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction.

5. What is the difference between a data processor and a data controller?
There are two different types of data-handlers the legislation applies to: 'processors' and 'controllers'. The definitions of each are laid out in Art. 4 of the General Data Protection Regulation. A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller. It was previously thought that GDPR applied mainly to data controllers, but it is clear that data processors are affected too.

6. Do businesses need to appoint a Data Protection Officer (DPO)?
DPOs must be appointed in the case of: (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data (Art. 37). If your organisation doesn't fall into one of these categories, then the organisation does not need to appoint a DPO.

7. What are Right of Access requests?
Right of access requests under Art. 15 of the GDPR provide individuals with the ability to know whether personal data about them is being processed by a data controller, and if so, what that information is and why it is being processed. The individual is entitled to a copy of the personal data in question and does not depend on whether someone is an employee, a worker or self-employed.

While both the GDPR contains exemptions, these mostly focus on questions of public interest, such as the investigation of crime or the maintenance of effective regulatory regimes.

Expert Insight

By Christiana Kouppi, G. Vrikis & Associates LLC

Recital 47 of the GDPR clearly states that fraud prevention is a 'legitimate interest' to process personal data:

"The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."

However, even for the purpose of fighting fraud, the controller still has to prove that legitimate interest applies and that the processing of personal data is necessary and unavoidable. They also have to balance the interest of fighting fraud with the interests, rights and freedoms of the people who the data applies to. The complexity of GDPR means that those who need to investigate fraud may face uncertainty regarding whether they need permission to proceed.

Observing the core principles of GDPR and preventing fraud at the same time it not an easy task.

8. What are the penalties in case of non- compliance?

Organisations can be fined up to 4% of annual global turnover for breaching GDPR or €20 million whichever is higher, which only applies to breaches that occurred after May 2018. This is the maximum fine that can be imposed for the most serious infringements, for example, not having sufficient customer consent to process data or violating core concepts. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

EU countries are now actively pursuing GDPR violators. France fined Google €50 million in January 2019 for its user consent and data policies, and the UK's regulator, the Information Commissioner's Office (ICO), fined Facebook £500,000 for serious data protection law breaches, Uber £385,000 for failing to protect customers' personal information during a cyberattack and Vote Leave £40,000 for sending out thousands of unsolicited text messages in connection with the 2016 Brexit vote.

Recently, the Information Commissioner issued a notice of its intention to fine British Airways an amount of £183 million for breaches of data protection law. The proposed fine involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers with approximately 500,000 customers being compromised. Investigations lead to conclusions of poor security arrangements by the Company, including the login, payment card and travel booking details.

9. What is consent?

GDPR defines 'consent' as: "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her."

GDPR imposes strict requirements upon data controllers who wish to rely on 'consent' as a legal basis for processing personal data. This does raise concerns in a number of areas, as the lines tend to become blurry; an example to refer to is the employment contract and, to the extent it cannot be relied upon as the legal basis for the processing of personal data.

Three key questions arise in this context:

- Is it an option to seek express consent outside the scope of the employment contract?
- If not, can a company rely upon" legitimate interests" as the legal basis to process that employee's personal data without seeking express consent?
- What about the individual's "right to be informed"?

In theory, employees could give their consent freely, independent of their employment contract, however, when there is a significant imbalance of power, such as between employer and employee, it is unlikely that consent will have truly been given freely.

10. How will GDPR and AML co-exist?

The right to erasure is clearly stipulated in the regulation, however, it is not an absolute right. There are exceptions including GDPR Article 17(3) (b) which imposes a difficulty as companies must retain customer due diligence and transaction records for a certain number of years after the relationship ends, even if the customer has requested to be forgotten. It remains to be seen how the industry will harmonise the regulations and exceptions in practice. **LM**

About Christiana and the Firm

Christiana Kouppi is the Partner and Head of Limassol Practice of G. Vrikis & Associates LLC a rapidly expanding and prominent law firm in Cyprus. The firm has been focused in providing high level legal advice to its clients and expanding its international profile and clientele, whilst at the same time maintaining a prompt, pro-active and family-office approach for its clients.

Contact

Christiana Kouppi
Partner
Phone: +357 25 261 777
Email: info@vrikislegal.com
www.vrikislegal.com

G. Vrikis & Associates Llc
ADVOCATES | LEGAL CONSULTANTS