KLOUDWERK

BRIEFING MEMO

DATA PROTECTION AND PRIVACY

Feeling overwhelmed by the onslaught of regulation? Confused by the streams of their acronyms? Frustrated about not being able to articulate their meaning? If the Global Financial Crisis taught us one thing, it is that prudential oversight was wholly inadequate. So, it's a safe bet that 10 years on, we've probably seen the thrust of what needed to be legislated, and now we learn to apply the regulations to our businesses accordingly.

> ***"The world is one big data problem."***
> ***– Andrew McAfee, MIT***

The last 10 years have seen businesses evolve through the opportunities afforded by the internet, where an underbelly of fascinating technology has been transformational. It would be quite a gamble to say how businesses will look in another decade's time from a tech point of view.

On the flipside, the bedrock of business regulation is set. We are interpreting and taking advantage of the new opportunities of regulation. We can't afford not to master their substance, so let's build some logic around their interrelationship. Welcome to the supervisory world and consumer protection in our electronic society.

The EU's data protection laws have long been regarded as a gold standard all over the world. The watershed moment sits around 2018 with real implementation actually becoming visible just this decade. There has been a veritable tsunami of regulation and you are justified in being overwhelmed by it all. GDPR, PSD2, MiFID II and IDD all hit in 2018.

Though each manifestly having their individual raison d'être, their singular common denominator is an explosion of personal data fields that need to be managed securely.

KLOUDWERK

GDPR

The EU **General Data Protection Regulation** (GDPR) was implemented in 2018 after a two-year notice period. It addresses how, in this digital age, data is stored, collected and transferred and applies to any enterprise that processes personal information of data subjects. Crucially, the new directive gives individuals control over their personal data and privacy. The key practical features are as follows:

- the activity of processing personal data is strictly defined;
- data controllers must design information systems with privacy in mind;
- data subjects have the right to request a copy of data collected; and, upon request, companies must erase personal data under "the right to be forgotten";
- companies who process personal data must appoint a data protection officer (DPO);
- data breaches must be reported to the authorities within 72 hours of detection;
- the transfer of the personal data of EU subjects outside of the European Economic Area (EEA) is forbidden, unless appropriate safeguards are imposed, or similar standards prevail.

No surprise, that the two-year implementation period was necessary. Enterprises needed to make significant investments in order to comply. **The biggest sign of readiness is having a data breach plan or incident response plan in place**. Failing to adhere to the GDPR has steep penalties, they are meant to bite. The threshold is the greater of €20 million, or 4% of a group's global annual turnover.

You can consult a live gallery of violations online at https://www.enforcementtracker.com/. For example, Google was fined a record £44m for failing to comply with GDPR, specifically by not obtaining adequate user consent for personalised advertising nor providing clear, easily accessible information about data collection and retention.

PSD2

The on-line activity that probably most touches data privacy are **electronic payments**. So GDPR goes hand in hand with the creation of a more integrated payments market. The revised EU **Payment Services Directive** (PSD2), entered force in 2018 however, unlike an EU Regulation (such as GDPR) which enters force on a given date for all EU members, the PSD2 is a **Directive**, leaving it up to domestic lawmaker to enact usually within a two-year timeframe. This means it started coming into effect across the EU throughout 2020 and since.

As the original Payment Services Directive (PSD) sought to regulate both the services and the providers, the up-date within PSD2 focuses on the payments industry from an **online** perspective. Crucially, it promotes the use of innovative online and mobile payments. It is substantially the start of a programme designed to open up banking data. It obliges big banks to release their customer data securely and in standardised form, so that it can be shared more easily between authorised organisations online.

You can see the obvious link to GDPR, but here it is about laying bare all the rich client information banks have been holding in a quasi-oligopolistic fashion. Making this information transparent allows for new product creation by competitors. In sum, the system makes it easier to view your finances overall, take out loans and other financial products, and pay for things on-line.

MiFID II & IDD

With GDPR and PSD2 having everything to do with personal data, other EU regulations have been equally demanding from a data point of view. The up-dated **Markets in Financial Instruments Directive** (MiFID II) regulates financial markets in the EU bloc and aims to improve investor protections. Rolled out in 2018, it replaces the pre-financial crisis directive. MiFID II not only covers virtually all aspects of financial investment and trading but also virtually all financial professionals within the EU.

MiFID II restricts the payment of inducements to financial advisors. Banks and brokerages must not charge for research and transactions in a single bundle. This forces both a clearer sense of cost and improves the quality of investor research.

Brokers will have to provide more detailed reporting on their trades, at least 50 more pieces of data, including price and volume information. They will have to store all communications, including phone conversations. It is worth noting that the UK financial markets had already enjoyed the substance of MiFID II via the Financial Conduct Authority's (FCA) Retail Distribution Review (RDR) which came into effect in 2012.

Of course, investment products reach beyond the asset management industry. Private pensions and life protection products are the remit of the **insurers**. So, think of the **Insurance Distribution Directive** (IDD), implemented in 2018, as nothing other than the MiFID II of the insurance industry. It aims to enhance consumer protection when buying insurance, including general insurance, life insurance and insurance-based investment products (IBIPs). It supports competition between insurance distributors by creating a level playing field and it imposes special disclosure requirements for products.

A rapidly expanding online data culture permeates GDPR, PSD2, MiFID II and IDD. Simply put, **the data you manage is no longer yours**. It belongs to the individual users of your services. Being a caretaker of data brings new responsibilities and threats of sanction. After all, it is only normal, if your organisation handles information related to a living and identifiable individual, then you have an obligation to protect that. **Are you?**

For further insights on this topic, please contact us via our homepage (www.kloudwerk.com)