PRIVITAR NTT DATA Global IT Innovator

The Key Things Your Whole Business Needs To Know To Be GDPR Ready

A whitepaper from NTT DATA and Privitar

Key Context

Timeline

The General Data Protection Regulation (GDPR) has been in development since summer 2012 and was adopted by the EU in April 2016. It is due to come into effect across the EU on the 25th May 2018. It will replace the EU Data Protection Directive from 1995, known as 95/46/EC. The GDPR can be read in full here: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Purpose

The GDPR cites rapid technological development (Recitals 6 & 7) as providing an impetus for an update on the 1995 directive, and the overriding intention to ensure privacy is uniformly protected across the EU.

However, the GDPR goes considerably further than just updating and ensuring ubiquity across the EU, it also fundamentally alters the balance of control over personal data between commercial organisations and individuals in a wide range of ways.

Regulation, not Directive

The GDPR is a Regulation, which, unlike the Directive it replaces, is enforceable as law as it is. For more information, see *Recitals 9 & 10*.

Scope

There are five questions you should ask to see how the GDPR might apply to the data you hold.

1. **Do you control personal data for commercial reasons?** Purely private activities are not within the scope of the regulation *(Article 2).*

2. **Do you control or process data?** This is a fundamental difference from the Directive GDPR replaces. As well as controllers, the GDPR also places obligations and restrictions on processors. A processor is a body which processes data under the instruction of a controller, an example might be a cloud provider who processes a controller's customer data, or an HR payroll provider who processes staff data.

3. **Are your data subjects EU citizens?** The Regulation broadens the territorial scope from the Directive and applies both if you're based in the EU and if you're a foreign company which offers goods or services to, or monitors the behavior of, EU citizens. This means that even in the event of Brexit, companies with European customers will still have to comply with the Regulation. For more information, see *Recitals 23 & 24* and *Article 3*.

4. **Is the data personal?** And if it is personal, how personal? While the GDPR applies to all types of personal data, the consequences of failing to comply varies based on the type of personal data involved. The definition of personal data now includes location, genetic, biometric and online identifier data, such as an IP address or cookie identifiers. For more information, see *Recitals 18, 30, 34 & 35* and *Article 4*.

5. **Is the data pseudonymized or anonymized?** Crucially, anonymized data is excluded from the remit of the GDPR (Recital 26)

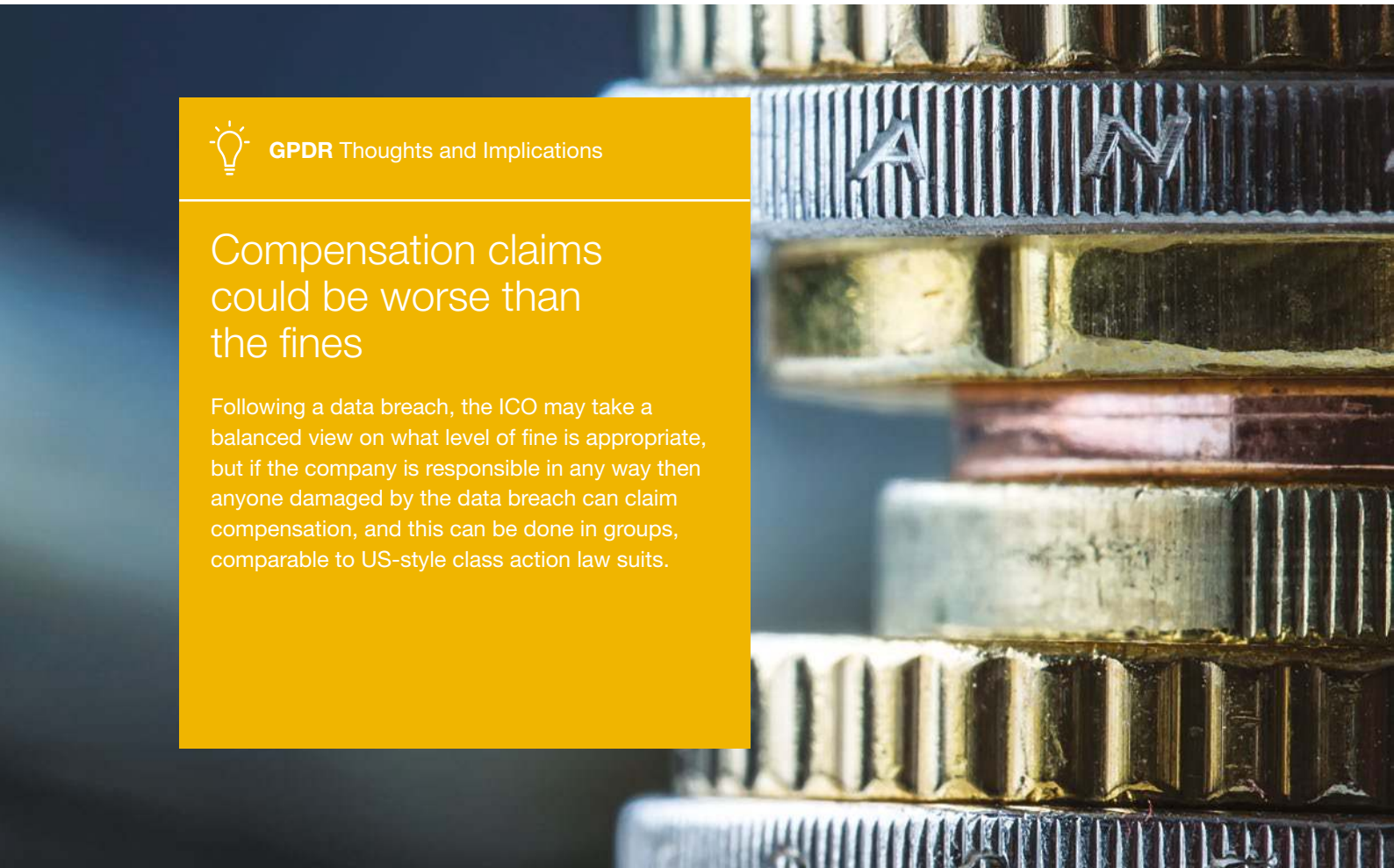
6 things you need to know

1 Administrative fines

One of the biggest changes of the GDPR is the change to the fines for non-compliance. Under the new regulation there will be two categories of fines, both of which are orders of magnitude larger than the current UK maximum fine of £0.5m.

Size	Up to 4% of annual global revenue, or €20m, whichever is higher.	Up to €10m or 2% of annual global revenue, whichever is higher
General areas *(broadly speaking)*	Interaction with customers, employees and authorities	Internal processes
Can be given for failing to comply with the rules on…	■ Gaining consent *(point 2 below)* ■ Upholding consumer rights *(point 3 below)* ■ Moving data out of the EU ■ Orders from a supervisory authority ■ Obligations under related national laws	■ Data protection by design *(point 4 below)* ■ Data breaches *(point 5 below)* ■ Employing Data Protection Officers *(point 6 below)* ■ Conducting Privacy Impact Assessments *(where relevant)* ■ Keeping appropriate records …and many more

For more information, see *Recital 148* and *Article 83*.



GPDR Thoughts and Implications

Compensation claims could be worse than the fines

Following a data breach, the ICO may take a balanced view on what level of fine is appropriate, but if the company is responsible in any way then anyone damaged by the data breach can claim compensation, and this can be done in groups, comparable to US-style class action law suits.

2 Consent has changed

GDPR fundamentally alters what constitutes consent for individuals. It requires organizations to rethink how they approach consent and explicitly rules out certain approaches, such as that currently used for cookies of taking inactivity as consent.

Four key changes to be aware of are:

Consent must be informed and unambiguous

Individuals must understand they're giving consent and demonstrate agreement, for instance with a clear affirmative action or statement.

Consent must be 'freely given'

The key here is that consent is not valid if the individual has not been given a genuine choice, so if an individual has to give consent to receive a service, unless the service cannot be provided without that personal data being collected, then that would likely not count as freely given consent.

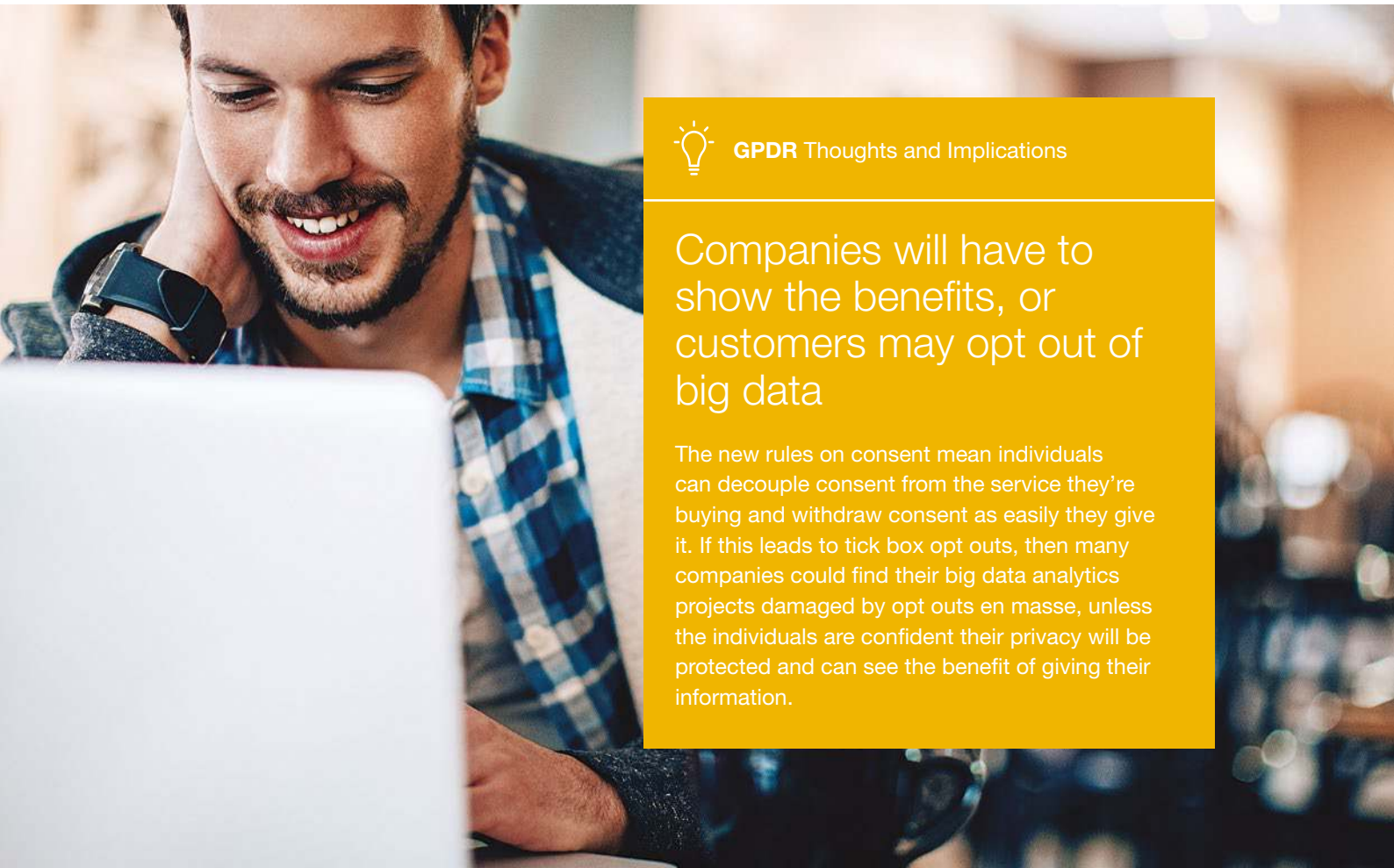
Consent must be as easy to withdraw as to give

This means if an individual is ticking a box to give consent, then they must be able to tick a box to withdraw consent, in the same way as is currently possible for direct advertising.

Consent is specific

Consent is requested for specific reasons and consent is then only valid for those specific reasons. This means that should an organization want to do something with collected data that they hadn't initially asked if they could do, then they would not be able to without asking for new consent.

When collecting consent, it is a controller's responsibility to notify an individual of their rights, e.g. their right to erasure. There are also some further significant changes around consent for children and the requirement for a higher burden of explicit consent for special categories of data, such as race, which should be carefully studied should you control or process special or children's information. For more information, see *Recitals 32*, *42 & 43* and *Articles 7, 8 and 13*.



GPDR Thoughts and Implications

Companies will have to show the benefits, or customers may opt out of big data

The new rules on consent mean individuals can decouple consent from the service they're buying and withdraw consent as easily they give it. If this leads to tick box opt outs, then many companies could find their big data analytics projects damaged by opt outs en masse, unless the individuals are confident their privacy will be protected and can see the benefit of giving their information.

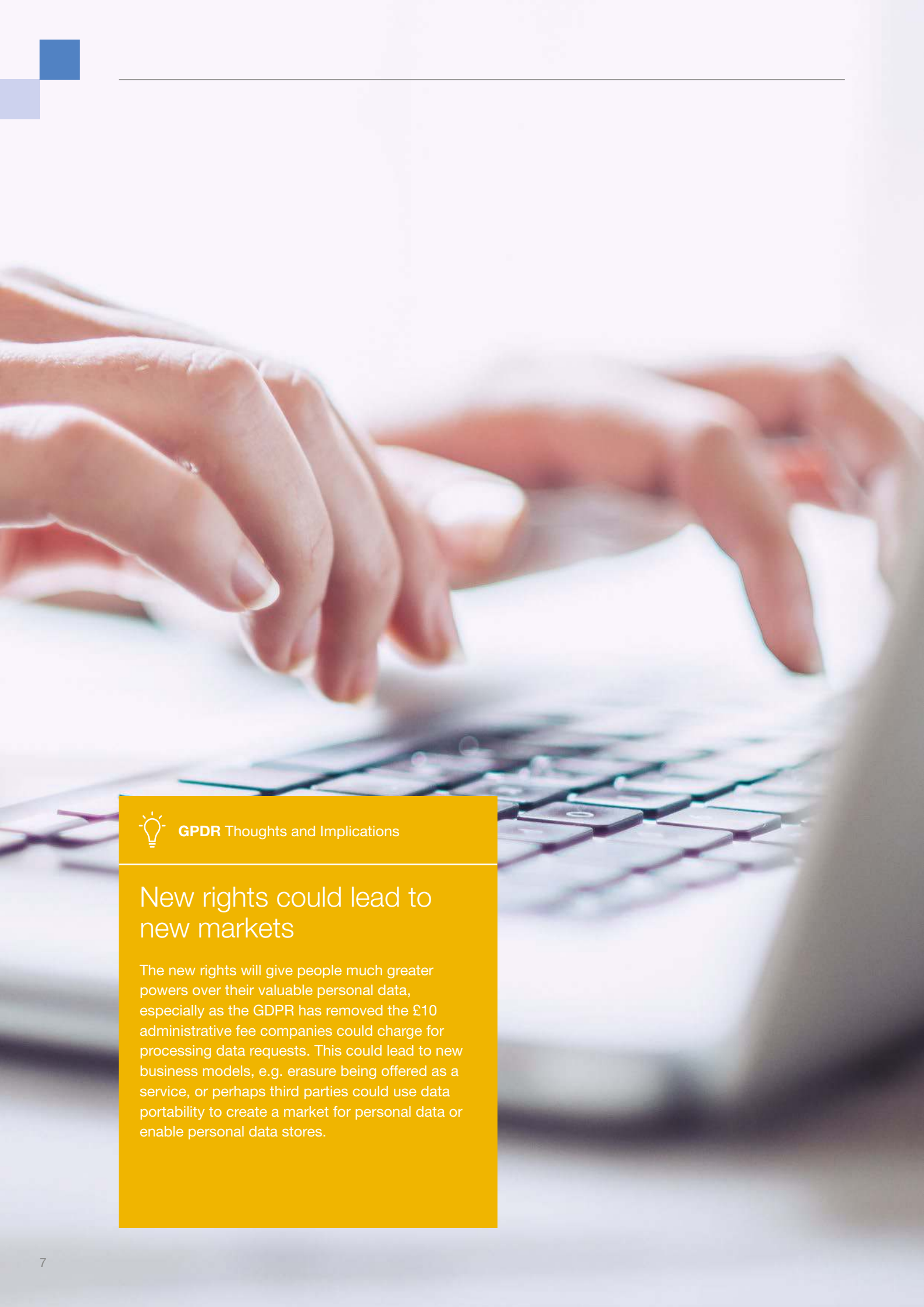
3 Individuals' rights have been strengthened and extended

GDPR introduces some new rights, and strengthens others. Sometimes these are building on existing laws or rulings since the Directive, like the 2014 EU Court decision of Spain vs Google, which established the right to be forgotten.

The rights enshrined in the GDPR are:

- Right to information on, and access to, personal data (Article 15). Individuals have the right to know if their personal data are being processed, and if so then to have access to that data.
- Right to rectification *(Article 16)*. Individuals have the right to correct or complete inaccurate or incomplete data.
- Right to erasure (or to be forgotten) *(Article17)*. Individuals have the right to have information on them erased, if, for instance, they withdraw their consent for their data to be used. Some of the consequences of this right are not entirely clear, as the right includes that if a controller has passed information on, or published it, then they must take 'reasonable steps' to notify other controllers of that data of the request for erasure.
- Right to restriction *(Article 18)*. If an individual has made a request which is pending, such as a request for erasure or correction, then the individual has the right for their data to be restricted such that no processing is done until the pending request has been resolved.
- Right to portability *(Article 20)*. Individuals have the right to have their data transferred, in an easy to use format, from one controller to another.
- Right to object *(Article 21)*. There are several areas where an organization balances its interests against the rights of an individual, and the individual has the right to object if they disagree with the decision. For instance, a controller may gather personal data without consent because they have a legitimate interest. Individuals have the right to object to their data being used on the basis of a legitimate interest. What constitutes a legitimate instance is not changed by GDPR and the Regulation cites examples such as fraud prevention (Recitals 47-50). For more information on what constitutes a legitimate interest see the Article 29 Data Protection Working Party paper from 2014: http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf
- Right against automated decision making, such as profiling (Article 22). Individuals have the right not to be subject to a decision based solely on an automated process if the individual will be significantly affected by the decision. This would rule out profiling for direct marketing.

For more information, see *Recitals 59-71* and *Articles 15-22*.



GPDR Thoughts and Implications

New rights could lead to new markets

The new rights will give people much greater powers over their valuable personal data, especially as the GDPR has removed the £10 administrative fee companies could charge for processing data requests. This could lead to new business models, e.g. erasure being offered as a service, or perhaps third parties could use data portability to create a market for personal data or enable personal data stores.

4 Data protection by design and default (aka privacy by design) is mandatory

GDPR mandates all organizations to adopt the principles of data protection by design. These principles originate in the 'Privacy by Design' (PbD) approach first put forward by Ontario's Information and Privacy Commissioner in the 1990s. PbD advocates building privacy considerations into projects from the start to mitigate privacy risks. An example of a PbD principle would be data minimization, which encourages controllers not to keep or collect data they do not need. For more information, see *Article 25*.

5 Data breaches must be reported within 72 hours

Until recently, organizations in the EU, unlike in the US, did not have to report data breaches. In the future, data processors will need to report data breaches to data controllers, who in turn will have to report data breaches to supervisory authorities within 72 hours. In instances where the data breach represents a high risk to the data subjects, the controller also has to notify those individuals. The controller is exempt if they've taken steps to ensure that the risk to the individual is mitigated, which can be achieved through the application of data protection by design principles where even in the case of a breach, the information lost is protected. For more information, see *Recitals 85-89* and *Articles 33 & 34*.

GPDR Thoughts and Implications

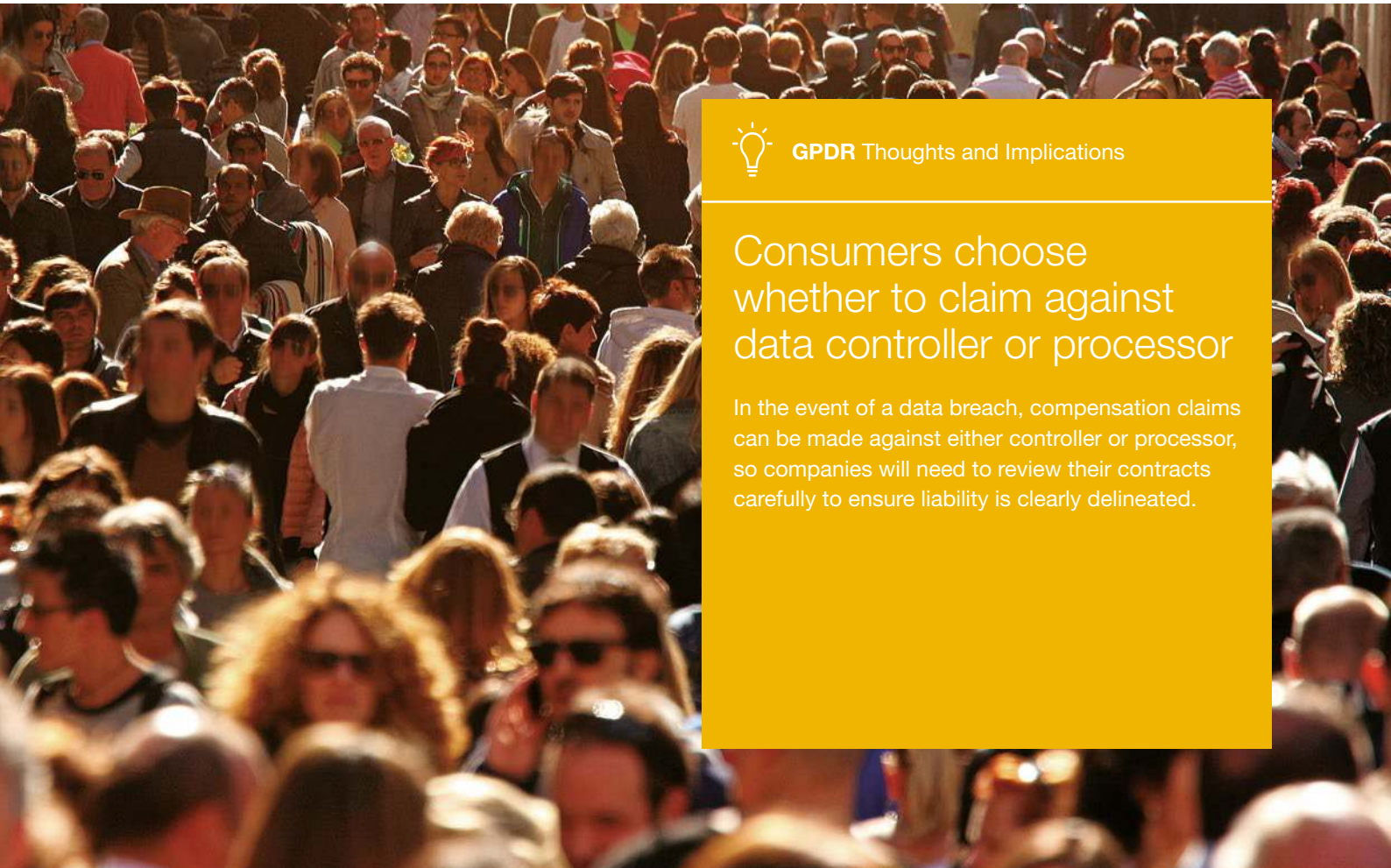
Compulsory data breach reporting may increase the cost of data breaches

In addition to requiring effective crisis response processes to be in place within organisations to meet the tight deadline, the change to compulsory reporting may increase the reputational damage done by breaches. This would continue the trend seen by the UK Government and PwC in their report last year which showed the cost of the worst data breaches nearly tripled between 2014 and 2015.

6 Data Protection Officers (DPOs) must be appointed

Organizations will need to appoint a DPO when their core activities regularly require the systematic monitoring of individuals on a large scale. The International Association of Privacy Professionals (IAPP) has estimated that Europe alone will require 28,000 DPOs. DPOs will be responsible for advising on, and monitoring compliance with, the GDPR and report to the organizations highest management level.

For more information see *Articles 37-39* and the IAPP's report:
https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/



GPDR Thoughts and Implications

Consumers choose whether to claim against data controller or processor

In the event of a data breach, compensation claims can be made against either controller or processor, so companies will need to review their contracts carefully to ensure liability is clearly delineated.

Achieve compliance with NTT DATA and Privitar

The time to act is now

Due to the scale of the changes GDPR requires, and the need to test solutions once implemented, companies must act now in order to ensure compliance by the deadline of 25th May 2018.

NTT DATA
Global IT Innovator

PRIVITAR

NTT DATA has led some of the world's largest data management projects, with proven tools and methodologies and expertise in relevant best practice.

Through a combination of technology partners and heavy investment in R&D NTT DATA is able to stay at the cutting edge and offer a very advanced and complete service.

NTT DATA's global model combines onsite, nearshore and offshore, thereby balancing accountability on a local level, with global reach and cost efficiencies.

Privitar enables organizations to mine and publish datasets containing sensitive information (e.g. customer data, patient records, banking transactions, geospatial coordinates, trade data) while preserving privacy and confidentiality.

This opens up data for safe secondary use while ensuring consistent and accountable protection of private information. Like security, privacy protection should be designed into data systems at every level, not bolted on as an afterthought.

Privitar adds a foundational privacy layer to your data processing architecture, enabling proper protection of confidential data.

Our partnership

To help companies manage the transition to the new GDPR regulation, we've combined NTT DATA's global experience and expertise in delivering data and process technology solutions, with Privitar's market leading privacy software. This allows us to offer a complete solution to GDPR compliance issues across different industry verticals from Financial Services and Telco through to the Public Sector.

Engage with us now for:

- A comprehensive assessment of your current compliance position and creation of a program of work tailored to your business priorities
- Planning and architecture remodelling to incorporate privacy-by-design principles in your modern data architecture
- Implementation of solutions that provide broader access and use of sensitive data assets with assured regulatory compliance

ABOUT

NTT DATA

NTT DATA is a leading IT services provider and global innovation partner head-quartered in Tokyo, with business operations in over 40 countries. Our emphasis is on long-term commitment, combining global reach with local intimacy to provide premier professional services varying from consulting and systems development to outsourcing.

www.nttdata.com/uk

ABOUT

Privitar

Privitar is an enterprise software company based on in London. The company's mission is to promote and facilitate the safe use of sensitive data assets. The company works with the world's largest organizations to drive benefits from data through broader use, collaboration and monetization without compromising on data privacy and security.

www.privitar.com