EU, Competition and Regulatory

April 2016

DATA PROTECTION HAS NEW TEETH:

SEVEN WAYS TO PREPARE NOW FOR THE EU GENERAL DATA PROTECTION REGULATION TO AVOID BEING BITTEN

On Thursday 14 April the European Parliament voted to approve the new EU General Data Protection Regulation (the Regulation), which overhauls a data protection regime dating from 1995. The Regulation makes some significant changes to the EU data protection regime which, perhaps most importantly, will now apply extra-territorially to data controllers and data processors alike. With large potential fines (the greatest of up to 4% of global turnover or €20 million) and a new maze of red tape, businesses should start now to make the necessary changes to their business practices in order to be prepared when the Regulation enters into force in early/mid 2018.

At the time of going to press, the Regulation has not yet been published in the Official Journal of the European Union (OJEU), although its publication is expected imminently. Once it is published it will enter into force two years from its publication date in the OJEU, which means that it is likely to "go live" in mid/early 2018.

The general principles of data protection will remain much the same, for example most of the definitions will be similar, as will the provisions on transfer of personal data outside of the EEA. However, the obligations on data controllers and processors will increase.

We discuss below seven of the main changes which will require action, and some immediate steps which businesses should take in order to deal with them. You can also find a brief overview of some of the main provisions of the Regulation in our client alert of December 2015[1].

1. Extra-Territoriality and Scope

Article 3 of the Regulation provides that the new regime applies to both data controllers and processors, located anywhere in the world, which either offer goods or services to data subjects in the EU (whether or not payment of the data subject is required) or monitor the behaviour of individuals within the EU. The Regulation has the potential to apply to the processing of personal data whether or not the processing takes place within the EU. The Regulation also applies to data

1 http://www.hfw.com/New-General-Data-Protection-Regulation-December-2015

controllers or processors established within the EU, regardless of whether the processing itself takes place in the EU, and to the processing of personal data by a controller not established in the EU but in a place where the law of an EU Member State applies by virtue of public international law, for example inside embassies or on board vessels or aircraft registered in an EU Member State.

The Regulation will not, however, apply to the processing of data by police and judicial authorities. This will be covered in a new Police and Criminal Justice Authorities Directive, which, at the time of going to press, is also yet to be published in the OJEU and will not be discussed below. Neither will the Regulation apply to activities outside EU law; common foreign and security activities; purely personal and household activity; or, generally, to EU institutions[2].

Action required?

To avoid potential fines and damage to reputation, businesses should audit their operations now.

- Do you offer goods or services to individuals within the EU?
- Do you use tracking technology (such as cookies) on websites which are aimed at individuals located in the EU?
- Are you subject to EU/EU Member State law because you have offices within the EU, or vessels or aircraft registered in an EU Member State?

If the Regulation may apply to you then it would be prudent to explore the potential impact of the Regulation on your business and operations as soon as possible.

2. Liability for processors as well as controllers (beware group claims)

The current data protection Directive only imposes liability on data controllers, the persons or entities which make the decisions on how and why personal data is processed. However, the new regime under the Regulation will impose obligations and liabilities on data processors as well[3]. Whilst the bulk of the obligations, and corresponding liability, will still fall on the data controllers, all businesses will need to comply with the rules - data processors will no longer be able to afford to be complacent.

This is a big change. Data processors will now be liable to enforcement action from data protection authorities, and open to claims from individuals where personal data has been processed illegally. Recital 146 provides that the controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation, although the processor should be exempt from liability if it proves that it is not in any way responsible for the damage. It specifically says that where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. It seems unlikely that the argument *'but I was only doing what I was told'* will be good enough to prove that a data processor is not "in any way responsible". In particular, data processors will also have separate responsibilities to ensure that personal data is kept secure[4].

The concept of "damage" is a broad one and will extend beyond financial loss. It is likely that as data subjects become more and more aware of their rights under the Regulation, and compliance becomes more onerous, group claims for breach of data protection law will become more common.

Action required?

If you have not previously considered the EU data protection rules because you only process personal data on behalf of others then this is the time to take stock, and advice, as appropriate.

If you are a data controller or processor (or joint controller), and you do not currently have data processing agreements with other relevant data controllers or processors of the personal data which you process, then you should put such agreements into place. Whilst previously the liability rested with data controllers, now both parties will be exposed if processing contracts are not used. In particular, consider the warranties which you will need in order to protect you from liability. For example, processors should consider requesting warranties that the data controller has obtained the personal data in question lawfully. Article 28 of the Regulation sets out the mandatory contents of such contracts.

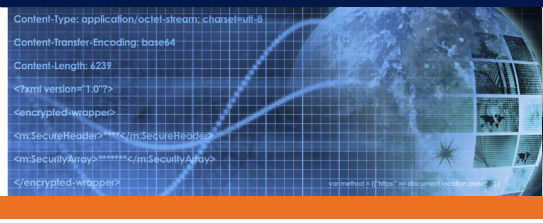
3. Record keeping and fair processing notices

With some exceptions, under the Regulation data controllers and data processors alike will have to comply with extensive record keeping and notification requirements.

As under the current regime, data subjects must be kept informed about the processing of their personal data.

2 Article 2
3 Article 3
4 Article 32





What is new is that there is a long list of information which must be included in these notices[5], although under Article 12 such communications must still be "concise, transparent, intelligible and easily accessible".

Both the data controller and data processor of personal data will be obliged to maintain, not just compile but also update, records of the processing activities under its responsibility. The records will need to be detailed, including for example the purpose of processing, data subjects and categories of personal data involved[6]. There is a specific obligation to cooperate with the supervisory authority, and to make such records available for inspection[7].

Where organisations have fewer than 250 employees the record-keeping requirements may not apply.

Action required?

Audit your personal data now.

- What personal data do you process?
- Why did you collect it?
- Why and how are you using it?
- Where is it kept?
- Do you have extensive personal data in archive?
- Do you still need it?
- Do you now use it for new purposes?

Once the Regulation comes into force there will be no phased implementation of the notification and record keeping requirements. If personal data is out of date or no longer needed, delete it.

You will save time and minimise risk by starting the data audit process now.

4. Right to object/freeze/remove personal data

The Regulation provides for more robust and enforceable rights for individuals.

Subject access rights have been strengthened – the information which must be provided to an individual who makes a genuine subject access request has been considerably increased[8] and the controversial "right to be forgotten" has been enshrined in Section 3 of the Regulation, on "rectification and erasure".

Individuals will also be entitled to object to their data being processed for the data controller's "legitimate interests", and an absolute right to object to their personal data being processed (including storage) for direct marketing purposes[9]. This is much stronger than the current right to object to receiving marketing emails and texts, because it affects what data about individuals is stored, not just what can be done with it.

Individuals will also have the right to request that their data be "restricted"[10]. This effectively means that a data controller will not be able to use the data in question until it has decided whether or not the individual's claim is genuine or can be refused.

Action required?

Consider putting processes in place, and designating a team of individuals, to deal with requests from individuals seeking to enforce their rights. The quicker that you can make a decision the sooner you can resume business and minimise the waste of company time and resources.

5. "Privacy by design" and Data Privacy Impact Assessments

An important new concept is that of "privacy by design" and by default[11]. When introducing new products, services, or processes, data controllers, though not processors, will need to show that the impact of such products, services or processes has been considered, and that steps have been taken to minimise any negative impact. Data should be pseudonymised where possible and should not be collected unless it is really needed.

Action required?

Do not collect personal data unless you can justify your purposes and you have conducted, and documented, privacy impact assessments. These should, amongst other things, determine how you will keep personal data safe. Make sure that your data protection policies are up to date and that your data processing is transparent.

6. Reporting of data breaches

Under Article 33, a data controller must notify a personal data breach to the relevant supervisory authority within 72 hours after becoming aware of a personal data security breach. The only exception to this is where the data breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Where there is such a risk, a delay beyond 72 hours must be accompanied by reasons for the delay. The contents of the notification are specified in Article 33. Under Article 34, when the personal data breach is "likely to result in a high risk to the rights and freedoms of natural persons" the data controller must notify the data subject "without undue delay".

5 Articles 13 and 14
6 Article 30
7 Article 31
8 Article 15
9 Article 21
10 Article 18
11 See Article 25


This could be a smaller notification window than 72 hours.

Data processors, under Article 33, must also notify the data controller, "without undue delay" after becoming aware of a personal data breach. This is likely to require fast, if not immediate, notification to the data controller.

Action required?

If you do not already have a cyber security breach procedure in place, consider creating one.

In the event of a security breach there will be very little time in which to determine the extent of the damage, the individuals affected, the security arrangements which will need to be either changed or strengthened, and whether or not the breach requires notification to the national data protection authority and/or individuals concerned. It would be prudent to establish parameters for making such decisions, and people who will be responsible for making them.

Also consider lining up public relations advisors who can help you to reduce the damage to your reputation.

7. Appointment of a Data Protection Officer

Although there will no longer be a need to register as a data controller in an EU Member State, data controllers and processors must designate a "data protection officer" in certain circumstances, set out in Article 37, including where:

1. *"the core activities"* of the controller or the processor consist of *"processing operations which... require regular and systematic monitoring of data subjects on a large scale"*.
2. The *"core activities"* of the controller or the processor consist of *"processing on a large scale"* of *"special categories of data"* (the new terminology for *"sensitive personal data"*) and *"personal data relating to criminal convictions and offences"*.

It is unclear at present whether this generally includes profiling activities, such as tracking technologies used to build up a marketable "picture" of a user's activities online, but presumably there will be guidance closer to the Regulation's implementation date.

In other cases, a controller or processor can choose to appoint a data protection officer, or a Member State can require it under local law.

Action required

Businesses should assess whether they will be required to appoint a data protection officer, and make arrangements accordingly.

Other changes – grounds for processing

Businesses should also note in particular that there are changes to the valid grounds for processing, such as the mechanisms and validity of "consent", and the concept of "legitimate interest", which has been greatly restricted. As explained above, privacy policies and information notices will need to be reviewed and updated.

Why should businesses care?

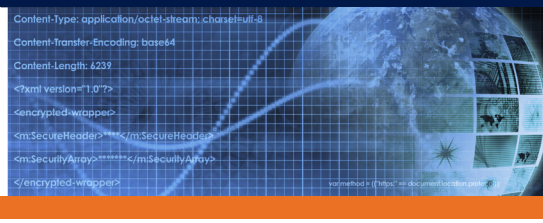
The penalties for getting this wrong are potentially very high.

Under Article 83, national supervisory authorities will have the power to impose fines of up to €20 million, or 4% of the total worldwide turnover of a business in the preceding financial year, whichever is higher. Member States must also lay down rules on other penalties applicable to infringements of the Regulation, and must take "all measures necessary to ensure that they are implemented... such penalties shall be effective, proportionate and dissuasive".

Although we presume that the maximum will only be awarded in the case of serious data breaches, we await guidance on their application from the supervisory authorities and the European Data Protection Board. We also do not yet know what "other penalties" Member States will impose once the Regulation comes into force.

In any event, it is safe to say that in drawing up this Regulation the Member States of the EU meant business. This is the product of four years of negotiation, drafts and redrafts of contentious clauses. The hefty fines provided for in the Regulation mean that it has real teeth. Attempts to match developing technology with appropriate regulation and enforcement is always difficult, but however the Regulation is enforced one thing is clear: data protection is here to stay.





For more information, please contact the authors of this briefing:

Anthony Woolich
Partner, London
T: +44 (0)20 7264 8033
E: anthony.woolich@hfw.com

Felicity Burling
Associate, London
T: +44 (0)20 7264 8057
E: felicity.burling@hfw.com

HFW has over 450 lawyers working in offices across Australia, Asia, the Middle East, Europe and South America. For further information about EU, Competition and Regulatory issues in other jurisdictions, please contact:

Daniel Martin
Partner, London
T: +44 (0)20 7264 8136
E: daniel.martin@hfw.com

Robert Follie
Partner, Paris
T: +33 1 44 94 40 50
E: robert.follie@hfw.com

Pierre Frühling
Partner, Brussels
T: +32 (0) 2643 3406
E: pierre.fruhling@hfw.com

Jeremy Davies
Partner, Geneva
T: +41 (0)22 322 4810
E: jeremy.davies@hfw.com

Jasel Chauhan
Partner, Piraeus
T: +30 210 429 3978
E: jasel.chauhan@hfw.com

Ian Chung
Partner, Dubai
T: +971 4 423 0534
E: ian.chung@hfw.com

Brian Gordon
Partner, Singapore
T: +65 6411 5333
E: brian.gordon@hfw.com

Guy Hardaker
Partner, Hong Kong
T: +852 3983 7644
E: guy.hardaker@hfw.com

Julian Davies
Partner, Shanghai
T: +86 21 2080 1188
E: julian.davies@hfw.com

Aaron Jordan
Partner, Melbourne
T: +61 (0)3 8601 4535
E: aaron.jordan@hfw.com

Stephen Thompson
Partner, Sydney
T: +61 (0)2 9320 4646
E: stephen.thompson@hfw.com

Simon Adams
Partner, Perth
T: +61 (0) 8 9422 4715
E: simon.adams@hfw.com

Fernando Albino
Partner, São Paulo
T: +55 (11) 3179 2900
E: fernando.albino@hfw.com

Lawyers for international commerce

hfw.com

São Paulo London Paris Brussels Geneva Piraeus Beirut Riyadh Kuwait Abu Dhabi Dubai
Singapore Hong Kong Shanghai Tianjin Perth Melbourne Sydney