

NEW GENERAL DATA PROTECTION REGULATION

Changes are afoot in the new year for data protection in the European Union, with the advent of the EU General Data Protection Regulation¹ (the GDPR).

The EU Data Protection Regulation

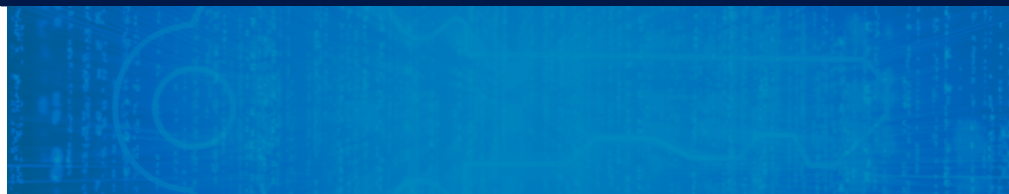
After years of tough negotiation between Member States, the text of the long awaited GDPR has been agreed by the European Parliament and Council. In talks on Tuesday 15 December, Member States' representatives agreed a compromise text. Subject to a positive final vote by the European Parliament in the new year, the Regulation will become law in approximately two years' time. The Regulation will be directly effective across all EU Member States, and the hope is that this will provide the "one stop shop" for data protection which will clarify the position in the EU. The precise wording of the draft may yet change, but the essence of the text should now remain as currently drafted.

Some of the key provisions of the GDPR are as follows:

1. Large fines and criminal penalties

Under the new regime, businesses could be fined up to €20 million or 4% of annual global turnover in the most recent financial year, whichever is greater. For infringements not subject to administrative fines, Member States have the power to set their own penalties, including criminal penalties. Under the current regime, Member States determine the fines, and/or criminal penalties, at local level. The UK data protection office, the Information Commissioner's Office, currently only has the power to impose fines of up to £500,000 for serious breaches. The much higher potential penalties under the GDPR will necessarily raise awareness of data protection obligations and encourage businesses to comply.

¹ Personal data protection: processing and free movement of data (General Data Protection Regulation) 2012/0011(COD).



2. **Extra-territorial applicability**

Businesses located outside of the EU will be subject to the GDPR if they offer goods or services to individuals located within the EU, or if they monitor individuals' behaviour which takes place within the EU, for example via cookies. This is a key change from the current regime and it is likely to make many more international businesses subject to the EU data protection regime.

3. **Application to controllers and processors alike**

Article 3 of the GDPR clarifies that the Regulation applies to the processing of personal data by both EU and non-EU controllers and processors. Currently the Data Protection Directive imposes the majority of its obligations on controllers only. This wider application, combined with the extra-territorial reach of the GDPR, increases exponentially the number of non-EU businesses which will need to be aware of the provisions of the GDPR and to comply with them. Allocation of responsibility between controllers and processors will become more relevant.

4. **“One Stop Shop” – lead supervisory authorities**

The GDPR aims to create a “one stop shop”. Where a certain processing activity affects data subjects in more than one Member State, the supervisory authority in the main establishment of the controller or processor, namely the country where the bulk of the data processing takes place, will act as a “lead supervisory authority” and will regulate that particular activity across the EU.



Subject to a positive final vote by the European Parliament in the new year, the Regulation will become law in approximately two years' time. The Regulation will be directly effective across all EU Member States, and the hope is that this will provide the “one stop shop” for data protection which will clarify the position in the EU.

FELICITY BURLING, ASSOCIATE

5. **Harmonization and the European Data Protection Board**

The GDPR encourages harmonization of its application and enforcement across the EU. Joint operations between supervisory authorities from different Member States will be encouraged “where appropriate” and a European Data Protection Board will be established to seek to ensure the consistent application of the GDPR across the EU. The Board will include representatives from each Member State, and its tasks will include issuing guidelines, recommendations, and opining on supervisory authorities' application of the GDPR. It will advise the Commission much as the Article 29 Working Party does under the current regime, but the new Board will have a separate legal

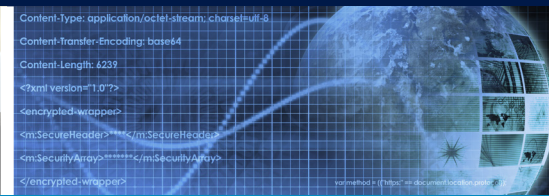
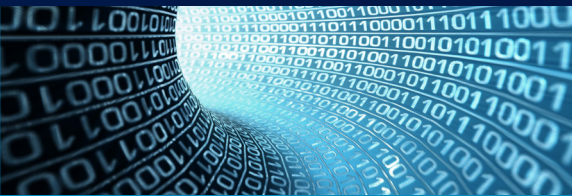
personality and will have the power to adopt binding decisions in disputes between Member State supervisory authorities.

6. **Registration as a data controller**

Registration as a data controller will no longer be necessary. However, data controllers and processors alike will need to maintain internal records of their data processing activities. Data controllers may also be required to carry out a “data protection impact assessment” before processing personal data.

7. **Processing children's data**

Member States were unable to agree on a proposal that parental consent will be required in order to process personal data of children under 13. The last minute compromise is that each Member State will be allowed under the



```
Content-Type: application/octet-stream; charset=utf-8
Content-Transfer-Encoding: base64
Content-Length: 6239
<?xml version="1.0"?>
<encrypted-wrapper>
<ms:SecureHeader?></ms:SecureHeader?>
<ms:SecurityArray?></ms:SecurityArray?>
</encrypted-wrapper>
```

Regulation to set their own limits for the age at which children no longer need parental consent. This can be set at any age between 13 and 16. This may drastically reduce young teenagers' use of social media, and create particular difficulties for global technology firms.

8. Requirement to notify breaches

The GDPR introduces a general data breach reporting requirement. Data controllers must notify personal data breaches to the competent supervisory authority, where feasible, not later than 72 hours after becoming aware of the breach, unless the data controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of the data subjects concerned. Notifications must also be made to data subjects "without undue delay" if the breach is likely to result in a high risk for their rights and freedoms.

Businesses should start to review their systems, contracts and policies now, and consider what changes will need to be made in order to ensure compliance once the Regulation goes live in two years' time. Businesses should assess the potential impact on individuals' privacy before starting new projects, and build privacy principles into the design of their operations. Failure to do so may leave businesses exposed to severe penalties as well as reputational damage.

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's London office is part of an international network of 13 offices in 11 countries. For further information about EU, Competition and Regulatory related issues in London or any other jurisdiction, please contact:

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

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

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

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

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

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

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

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

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

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

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

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

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

Lawyers for international commerce

hfw.com

© 2015 Holman Fenwick Willan LLP. All rights reserved

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice.

Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please contact Craig Martin on +44 (0)20 7264 8109 or email craig.martin@hfw.com

São Paulo London Paris Brussels Geneva Piraeus Dubai Shanghai Hong Kong Singapore Melbourne Sydney Perth