EU Data Protection Reform: Where are we – and what can you do to prepare?
Introduction

What’s going on?

It is nearly three years since the European Commission unveiled its ambitious plans for overhaul of the data protection regime in the form of the draft General Data Protection Regulation (the “Regulation”). As we approach the end of 2014, although various adoption target dates have come and gone, the reform has nevertheless reached a significant milestone – approval in March 2014 by the European Parliament (EP) of a significantly amended text – and the Council has reached a “partial general approach” on certain key aspects of the Regulation.

Why are we waiting?

However, based on its approach that “nothing is agreed until all is agreed”, the Council still has significant work to do before the Regulation can enter its final critical phase – namely closed-door “trilogue” negotiations between all three EU institutions to hammer out a final compromise text. The new Commission President has tasked the new Commissioners who now share responsibility for the DP portfolio with steering the Regulation to adoption by May 2015. Italy, the latest Member State to hold the Council Presidency, has (like the Greek Presidency before that, and the Irish Presidency before that) declared DP reform to be a priority. If the latest target adoption date of May 2015 is met, and if the proposal remains in the form of a directly effective Regulation (instead of a Directive requiring transposition), the new rules could be in force as soon as May 2017.

What does this mean for me?

It remains to be seen whether that timetable will be achieved. With so many issues in the Regulation still the subject of negotiation, and in many cases, further technical work, it is impossible to say what the wide-ranging new regime will look like in every detail when the legislators finally complete their work. What is certain however is that overall, the new regime will be more onerous – and that the sanctions for breach will be drastic, with proposed fines of up to 100,000,000 euros or 5% of an enterprise’s global annual turnover.

So, now what?

In this update Olswang’s award-winning data protection team select some of the key components of the proposed Regulation, compare these to current data protection laws, summarise the current state of negotiations and comment on the likely practical implications for business.

Ross McKean, Partner
Head of Data Protection
Olswang LLP

www.olswang.com/eudataprotectionreform
# The Top 12 Issues

<table>
<thead>
<tr>
<th></th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Fines and enforcement</td>
</tr>
<tr>
<td>2.</td>
<td>Territorial reach</td>
</tr>
<tr>
<td>3.</td>
<td>Scope of personal data</td>
</tr>
<tr>
<td>4.</td>
<td>Justifications for processing</td>
</tr>
<tr>
<td>5.</td>
<td>Data Protection Officers and Governance</td>
</tr>
<tr>
<td>6.</td>
<td>Security and breach notification</td>
</tr>
<tr>
<td>7.</td>
<td>Processors and supply chain</td>
</tr>
<tr>
<td>8.</td>
<td>Profiling</td>
</tr>
<tr>
<td>9.</td>
<td>Data portability</td>
</tr>
<tr>
<td>10.</td>
<td>The Right To Be Forgotten</td>
</tr>
<tr>
<td>11.</td>
<td>International Transfers</td>
</tr>
<tr>
<td>12.</td>
<td>Privacy by design</td>
</tr>
</tbody>
</table>
1. Fines and Enforcement (Articles 79 and 63)

With fines of up to 5% of global annual turnover proposed, the new regime will put data protection on a par with anti-trust and anti-bribery sanctions. "Taking a view" on data protection compliance is likely to become prohibitively expensive. There is a great deal for organisations to do between now and 2017.

What is the current law?

A recurring theme of the current data protection regime is that there are wide differences both in substantive laws, sanctions and enforcement activity among the different Member States. The current Directive 95/46/EC (the "Directive") leaves a lot of discretion and detail down to the individual Member States; including sanctions. For the large part, current sanctions are limited; certainly when compared to the likes of financial services, competition / anti-trust and anti-bribery regimes. An organisation would have to do something pretty bad under the current regime to end up with a small fine in the hundreds of thousands of euros. One of the most effective tools in the EU data regulators' armoury today is the threat of public censure.

What will change under the Regulation?

Sanctions are the real game-changer under the proposed Regulation. The rights and duties proposed by the Regulation have to be viewed through the powerful magnifying glass of the proposed sanctions and enforcement regime. "Taking a view" on data protection compliance is likely to become prohibitively expensive. For starters, the Regulation sets out the sanctions regime, rather than leaving it down to each Member State. The proposed maximum fines are huge: the text of the European Parliament (the "EP") proposes fines of up to 100,000,000 euros or 5% of global annual turnover; more than double the Commission's original proposal of 2% fines.

Comment and practical advice

Whatever the final form of the Regulation, it is reasonably certain that sanctions will be much greater. There is a short window of opportunity over the next two to three years before the Regulation becomes law. There is a lot to do and it is increasingly difficult to find good resources to support data protection compliance with the ongoing arms race among organisations and advisors for data protection talent. The advice is simple: Don't delay; the clock is ticking. You need to comply.
The new regime will greatly extend the reach of the EU legislation to Silicon Valley and beyond. Non-EU controllers will also need to appoint representatives in the EU.

What is the current law?

"Does EU data protection law apply to me?" is not a straightforward question to answer under the current regime due to differences in approach among the Member States and the recent CJEU decision in the case of *Google Spain v AEPD and Costeja Gonzales*. Data protection laws engage under the Directive (a) where processing is carried out in the context of the activities of an establishment of a controller on the territory of a Member State; or (b) if the controller is not established in the EU but uses "means" or "equipment" on the territory of that Member State, save for pure transit. It is common for non-EU controllers to try to exclude the application of EU laws by ensuring that they have no establishment or means or equipment in Europe. The *Google Spain* decision has cast doubt on this strategy. Europe's highest court, the CJEU, held that the sale by Google's Spanish affiliate of advertising offered by Google Inc. on the Google search engine was "in the context of the activities" of Google Inc. and that Google Inc. was established in Spain and therefore subject to EU data protection laws.

What will change under the Regulation?

It is reasonably certain that controllers and processors that process personal data in the context of the activities of an establishment in the EU will be subject to the Regulation. This is similar to the first limb of the current test in the Directive, the difference being that processors will now also be caught by the Regulation. The Regulation proposes ditching the Directive's "means / equipment" test. In its place, the Regulation will likely engage on non-EU controllers where either (a) they are offering goods or services (whether or not payment is required) to data subjects in the EU; or (b) they are monitoring their behaviour (within the EU). According to Recital 20 of the Council's agreed text, to determine whether a non-EU controller is "offering goods or services", the facts need to be considered in the round. Mere accessibility of the website, or email and contact details or using a language which is generally used in the third country where the controller is established, aren't enough. On the other hand, factors such as offering languages and currencies generally used in one or more Member States with the possibility of ordering in that language, or mentioning customers in the EU would make it more likely that the controller is held to be offering goods or services to the EU and therefore subject to the Regulation. The draft Regulation also proposes to strengthen the requirement for non-EU controllers to appoint a representative within the EU.

Comment and practical advice

Non-EU controllers (and potentially non-EU processors, depending on where the final text lands) doing business in the EU with EU data subjects’ personal data should prepare to comply. It remains to be seen how effective the enforcement of these provisions will be against non-EU entities. Resources of regulators are finite and enforcing against controllers outside of the EU is more challenging and expensive than enforcing within the EU. However, given the huge proposed fines, if you are offering goods or services to EU customers or monitoring their data, the practical advice is that you need to take steps to demonstrate compliance.
3. Scope of Personal Data (Article 4)

The definition of personal data is set to broaden under the Regulation, bringing much more data into the regulated perimeter. Changes are proposed to keep pace with the online environment and rapid technological change.

What is the current law?

The Directive defines personal data as "any information relating to an identified or identifiable natural person [...] who can be identified, directly or indirectly, in particular by reference to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Recital 26 of the Directive states that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". The latter wording has been interpreted by some Member States (e.g. the UK) to narrow the definition of personal data, focusing just on the controller's means to identify an individual and not considering whether the data could be linked to an individual by "any other person". Other Member States have opted for a more expansive definition, leading to a patchwork of different approaches.

What will change under the Regulation?

The Regulation will establish a single broad definition of personal data for the whole of the EU. What is fundamental to note is that the concept of identification will likely no longer be limited to the possibility of knowing the address, name, etc. of an individual, but rather will focus on the likelihood of "singling out" an individual whether directly or indirectly (Recital 23 of the EP's proposal). The latest text from the Council, which remains subject to discussion, defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical physiological, genetic, mental, economic, cultural or social identity of that person". The reference to online identifiers would cover, for example, cookies and IP addresses when used to track specific users. Under the Council's text, anonymous information - not relating to an identified or identifiable natural person or data rendered anonymous - so that the data subject is not or is no longer identifiable - falls outside the scope of the Regulation. Information on deceased persons would, in principle, also be excluded, unless it impinges the interests of data subjects.

Comment and practical advice

The clear direction of travel in negotiations for the final text of the Regulation is for an expansive definition of personal data capturing cookies, IP addresses, web beacons and other tracking technologies when used to track an individual. To mitigate compliance risk, organisations should, first, effectively implement data minimisation and ensure that only that data necessary for a legitimate purpose is collected and processed – and no more than that. Secondly, if there is any doubt as to whether data is personal data, the prudent approach is to treat it as such. Thirdly, personal data should be stored no longer than necessary for the purpose or purposes for which it was collected; then it should be securely wiped in accordance with a documented retention policy. Fourthly, wherever possible, personal data should be aggregated and anonymised so that it is no longer personal data.
The new regime is based on the existing grounds to justify processing in the Directive. However, there are proposals for a much stricter test for consent and a significant narrowing of the "legitimate interests" justification. Taken together, this would make it harder to justify processing compared to the current regime. There is also debate as to the extent Member States will be allowed to pass national legislation to fine-tune justifications in specific sectors such as employment, health and journalism.

What is the current law?

In the absence of valid consent, personal data may only be processed under the Directive (i) if it is necessary for the performance of a contract to which the data subject is party or to comply with legal obligations or for the protection of the vital interests of the data subject, (ii) if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or (iii) if necessary for purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interest of the fundamental rights and freedoms of the data subject. Additionally, other exceptions for special cases and sectors exist. Processing of special categories of data (i.e. sensitive personal data) is subject to stricter rules.

What will change under the Regulation?

The Regulation is similar to the current regime, though there is a proposed raising of the bar and narrowing of several justifications. The Commission had suggested granting power to the Commission to adopt "delegated acts" that give more meat to certain vague and abstract provisions on justification. However, this proposal has now been rejected by the Council and also the EP.

Moreover, Member States would be empowered to pass national legislation in certain sectors (e.g. employment, journalism and health). The list of sectors is still under discussion between the EU institutions. The Council and EP seem to favour a wider and longer list also including, for example, data processing for statistical, archival or social purposes. Regarding legitimising conditions for direct marketing and for cookies, the relevant Directives (Directive 2002/58/EC and Directive 2009/58/EC) would be carved out from the scope of the new Regulation, i.e. these Directives and their national implementing laws would remain in force.

Significantly, major changes are proposed to the specific rules for obtaining valid consent. Consent must meet strict criteria to be valid, including a clear layout for the consent document and the specific language or content of such consent. In addition, the EP's text suggests providing for consent to have an "expiry date" (Article 7).

Comment and practical advice

The new regime is likely to look similar to the current Directive's approach to justifying processing. However, it is significantly more restrictive, notably by raising the bar for consent and by narrowing the scope of the "legitimate interests" justification. This may not be all that significant for German data controllers, who live with stricter rules already, but it will require a much tighter focus on justification in the UK, which currently enjoys a far more permissive regime.
5. DPOs and Governance (Articles 28, 35-38)

There has been much debate as to whether organisations should be required to appoint a DPO and incur significant cost, or if the current voluntary approach should continue.

What is the current law?

The current Directive includes a non-mandatory option for Member States to provide for simplification of, or exemption from, notification requirements by appointing a data protection official to ensure internal data protection compliance and to keep a register of processing operations.

What will change under the Regulation?

**DPOs:** The duty to appoint a DPO has been heavily debated ever since the publication of the first draft of the Regulation. The Member States' positions could not be more diverse. In some Member States, every proposed amendment has been a dilution of the original proposal. For data controllers established in several Member States, the appointment of DPOs will represent a significant administrative and financial investment, relative to the current regime.

There have been several changes to the relevant provisions in the different institutions' drafts. The [Commission's original text](https://www.olgswang.com) obliges data controllers to designate a DPO if the data processing is carried out by an enterprise which has 250 or more employees. The [EP's version](https://www.olgswang.com) would raise the threshold by obliging data controllers to designate a DPO if the data processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period. The Council's revised text in contrast would make the designation of a DPO non-mandatory, except where required by European Union or Member State law. The EP's version also extends the tasks of the DPOs, to include e.g. informing employee representatives about data processing relating to employees. The Council has, on the other hand, deleted several tasks.

**Governance:** The Regulation introduces a number of new governance requirements. The Commission's original text obliges data controllers to carry out impact assessments for certain higher-risk processing (Article 33). The EP's version only requires an impact assessment if a mandatory risk assessment (Article 32a) indicates any "specific" risk. These higher-risk areas include (in the EP's extended list): data processing relating to more than 5000 data subjects during any consecutive 12-month period; the processing of sensitive data; or processing operations which contain a risk by virtue of their nature. In some cases there is also a duty to consult the supervisory authority prior to the data processing (Article 34). The EP's version enables data controllers to carry out the prior consultation with the DPO (if there is one) instead of the supervisory authority. In addition, the EP's version obliges data controllers to assess the impact assessment on a regular basis, at least every two years. The Council's version, being more risk-based, requires a "high" risk to trigger the implementation by the controller of a mandatory personal data impact assessment, allowing certain leeway to supervisory authorities to determine a public list of processing operations not requiring an impact assessment, except in cases where it is expressly required by the Regulation. In terms of record-keeping and red tape, Article 28 of the Commission's draft proposes requirements for the controller and processor to document the detail of the processing. The Council's version is similar, while the EP's version of the Regulation is lighter-touch and has deleted several of these record-keeping duties.
Comment and practical advice

It is still uncertain whether data processing entities – data controllers and data processors – will have to designate a DPO and what the threshold will be. Data controllers are likely to have to carry out assessments to analyse and minimise the risks of their data processing operations and the impact on data subjects. It will be interesting to see what tasks and competences are left with DPOs in the final Regulation, and whether the relevant assessments can be carried out without a DPO. It is also unclear how extensive the obligations to document data processing will be in the final version, but it is certain that overall data controllers will have greater administrative burdens and costs - despite the fact that some existing red tape, such as notification duties and prior checks, may be abolished.
6. Security and Breach Notification (Articles 30-32)

The introduction of data breach notification looks certain, although important questions remain about the materiality thresholds and deadlines. The broad requirement for "appropriate" security will be extended to apply to processors as well as controllers, although it is unclear how prescriptive the detail of the final Regulation will be.

What is the current law?

**Security:** The Directive requires controllers to ensure that "appropriate" technical and organisational measures are implemented to protect personal data, having regard to the state of the art and the cost of their implementation; such measures are required to ensure a level of security appropriate to the risks and the nature of the data. In addition to the Directive's core requirements, various Member States have specified specific security measures which must be put in place by a controller when appointing a processor. The detail of these measures varies between the different Member States.

**Data breach notification:** There is no express obligation to notify data breaches under the Directive, though there are some sector specific requirements such as those applicable to communications providers and ISPs under the E-Privacy Directive. In addition, some Member States, for example Germany, have imposed broader data breach notification requirements.

What will change under the Regulation?

**Security:** All three institutions support the principle that processors as well as controllers should be directly liable for implementing "appropriate" technical and organisational security measures, having regard to the state of the art and cost. However, there is a spectrum of proposed approaches, with the EP's stance being the most prescriptive and that of the Council being the most risk-based. The Commission's text requires controllers and processors to make an evaluation of the risks, the EP's text requires a formal privacy impact assessment in certain cases (Article 32a (2) (a) to (h)), while the Council's text simply requires a risk assessment which takes into account "the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risks" to the data. The EP's text mandates specific issues to be addressed in such a security policy including integrity, confidentiality, availability and testing. All three institutions' texts allow for more detailed guidance or compliance benchmarks in some form, whether via Commission "implementing acts" (the Commission's proposal), via guidance from the new EDPB (the EP's proposal) or through compliance with approved codes of conduct or certification mechanisms (the Council's position).

**Breach notification:** There is also consensus on the principle that data breaches should be notified to the regulator and, where the breach puts individuals' data at risk, to data subjects. But again, there is a wide spectrum of approaches proposed. The Commission's proposal on notifying regulators was criticised both for its lack of any materiality threshold, and for its unrealistic 24 hour deadline. The EP's stance relaxes this to notification "without undue delay" within a target of 72 hours (Recital 67) and provides expressly for information to be provided to the regulator in phases and introduces a materiality threshold of breaches which may result in "physical, material or moral damage". It adds a requirement for regulators to publish a register of the types of breaches notified. The Council's position is, again, more risk-based: the target notification time remains 72 hours, but the threshold for breaches which need to be notified to the regulator and to individuals is the same, namely breaches "likely to result in a high risk" to the individual's rights and freedoms e.g. "discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant


oger or social disadvantage”. Regarding notification to affected individuals, both the Commission's and EP’s texts set the threshold lower, at breaches "likely to adversely affect" the person's personal data or privacy.

**Comment and practical advice**

**Security**: The Regulation changes compliance risk fundamentally for data processors, who will be directly liable for breach of the expanded security obligations for the first time. Sourcing and supply chain arrangements will need to be reviewed to ensure they are fit for purpose for the new regime (see section 7 of this update).

**Breach notification**: Even if the final Regulation reflects the Council’s risk-based approach, data controllers and processors will need to gear up in order to notify data breaches within an exacting (and still unrealistic) 72 hour deadline. Data protection regulators – and the public – could find themselves suffering from notification fatigue unless the Regulation and any related guidance strike the right balance between the need for disclosure of serious breaches on the one hand and the risk of breach notification overload on the other. With the increasing risk of cyber-attack and the serious harm that can be caused to individuals whose data is compromised, it is inevitable that some of the highest fines under the new Regulation will be reserved for controllers and processors who are found wanting against the proposed exacting security standards of the Regulation. Security, from collection to secure deletion, should be a top priority for organisations when addressing data compliance. For larger organisations, there is a pressing challenge to build data breach investigation, categorisation, containment and response infrastructure, ideally within the cloak of legal privilege. Data breach and crisis policies should be drafted and road-tested.
Exposure to data-related liabilities - for both customers and suppliers - will increase. With the Regulation potentially taking effect in 2017, new deals being negotiated now need to be future-proofed. Parties to contracts will need to document their data responsibilities even more clearly and the increased risk levels will impact negotiations on security standards, risk allocation and pricing.

What is the current law?

In general, obligations under current EU data protection laws only apply to controllers. Controllers are required to ensure that processors provide sufficient guarantees as to security, keep data secure and only process in accordance with the controller's instructions in a written contract; however these obligations generally apply solely to the controller who then passes them down the supply chain to their processors. Multi-nationals with affiliates (controllers) in multiple Member States often have to flow down quite different security and related obligations to processors, depending on which Member State's law applies, adding cost and complexity to the supply chain – without arguably adding any greater protection for the data subjects concerned.

What will change under the Regulation?

The proposed Regulation introduces a fundamental shift in liabilities, with processors for the first time subject to a number of obligations and restrictions, and exposed to fines and other regulatory action. There appears to be broad consensus (give or take some nuances in the detail) between the three institutions on the following proposed principles: a controller must use a processor providing sufficient guarantees as to security (Article 26); additional mandatory terms will need to be included in processor contracts (Article 26); both the controller and processor will be responsible for appropriate security, based on a joint evaluation (or impact assessment) (Article 30); compromise on the possibility of making use of sub-contractors under certain conditions (Article 26); a requirement for the details of the processing to be documented (Article 28); processors must comply with the data export principle and adequacy mechanisms (Article 40); processors must alert and inform controllers immediately (or without undue delay) after the establishment of a data breach (Article 31). Points which still need to be discussed during trilogue negotiations are: whether or not a processor will attract liability as a joint controller if it acts outside the controller's instructions (Articles 26 and 27, which have been deleted in the Council's proposal); and whether or not it will be mandatory for processors as well as controllers above a certain threshold to appoint a DPO (Articles 35-37).

Comment and practical advice

The increased obligations and shifts in liability, combined with the potential exposure of both customers (controllers) and their suppliers (processors) to massive fines, will have a profound impact on supply chains. They will impact every stage of the procurement process and every link in the chain, from supplier and sub-contractor selection to pricing and from negotiation of the contract to ongoing governance. Suppliers (as processors) will no longer be able to pass legal responsibility for determining security requirements to their customers (as controllers) as the Regulation proposes that this should be a joint responsibility. It is common for suppliers to cap contractual liability to their customers for security breach; however, these caps are unlikely to provide any defence to a regulator imposing a fine directly on the supplier. For customers, the practical advice is to select suppliers who process personal data with care and to document due diligence, using a privacy impact assessment if appropriate. Contractual governance
and audit should be used to ensure ongoing compliance. For suppliers, business cases for legacy and new deals will need to be reassessed to factor in increased compliance risk. Costs will need to be calculated both for improved security and the increased risk of fines and appropriate change control provisions included in the contract to address the change in law once the Regulation has been finalised.
8. Profiling (Article 20)

The scope of the concept of profiling remains subject to further debate. The outcome of these discussions will be critical for advertisers, insurers, employers and other sectors which rely on the ability to profile individuals.

What is the current law?

The Directive grants the right to individuals not to be subject to a decision producing legal effects or significantly affecting them, which is “based solely” on automated processing of personal data intended to evaluate personal aspects of the data subject (such as performance at work, creditworthiness, reliability or conduct) (Article 15). It is worth bearing in mind that the Directive’s rules on profiling were drafted long before the advent of big data and the increasingly sophisticated profiling technology now used extensively in the advertising, insurance and financial services sectors.

What will change under the Regulation?

The EP has proposed a broader definition of “profiling” as “any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behaviour”. The Council’s proposal also includes a definition of profiling as a form of automated processing. One major shift compared to the Directive is with respect to the legal grounds on which profiling could be justified with the introduction of a consent-based approach for profiling which “produces a legal effect” or “significantly affects the data subject” effectively ruling out this type of profiling for big data solutions given the practical compliance challenges of achieving the exacting requirements for consent under the draft Regulation. Other less invasive profiling may be easier to justify, provided information is given to the data subject and an opt-out is provided.

Comment and practical advice

For data analytics driven businesses relying on the ability to build profiles on individuals, the further discussions on this topic are crucial and in particular where the line will be drawn between on the one hand profiling that can be undertaken without consent (provided information and an opt-out is provided) and profiling requiring consent. The treatment of advertising technologies is currently unclear. Any move to a requirement for consent would be challenging to implement making it very hard to offer relevant and targeted adverts to users.
9. Data Portability (Article 18)

The introduction of a right to data portability now looks more likely than not in some shape or form, however there is much discussion around how to make it workable in practice, and whether it sits more comfortably in competition and/ or intellectual property law rather than data protection. Some argue the concept has little to do with data protection at all and will lead to disproportionate compliance cost in markets which do not suffer from customer lock-in.

What is the current law?

The current Directive has no equivalent concept of data portability. Some argue it has little to do with data protection at all.

What will change under the Regulation?

Article 18(2) of the Commission's proposal introduced a new concept of data portability, a right that would enable data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller. The detail of those electronic formats and the practicalities of such transfers would be fleshed out by the Commission in implementing acts (i.e. delegated legislation). The EP's amended text merged the portability right into Article 15, renaming it the less-catchy "right of access and to obtain data for the data subject". The amended text provides that where personal data is processed by electronic means, a data subject has the right to obtain a copy of their personal data in a "commonly used", "electronic and interoperable" format without hindrance from the data controller. However, the amended text has limited the scope of the portability right so that if a data subject requests a transfer of data, the controller would only transfer the data direct to the other controller where such a transfer is "technically feasible and available". The EP also made other qualifications and exceptions to portability. The latest Council official text has proposed further limitations to the right to data portability and confirms that there are still significant differences among the Member States on the structure of this right.

Comment and practical advice

Data portability is one of the most controversial proposals in the draft Regulation, with various Member States querying whether it would not be better addressed in consumer or competition law. There is concern that forcing controllers to transfer personal data may require disproportionate cost and effort – particularly in markets where there is no consumer "lock-in" - and might compromise valuable proprietary information and intellectual property. Other issues that have been raised by Member States' delegations include concerns around certain industries such as healthcare, where data portability may endanger ongoing research or continuity of services; and concerns that the portability right may be difficult to apply in cases where a certain data involves multiple data subjects who disagree on the transfer. For now, it is fair to say the issue of data portability obligations under the new Regulation is a moving target.
10. The Right to be Forgotten (Article 17)

Data subjects' rights to erasure of information (formerly known as the 'right to be forgotten') will form a central part of the new Regulation. However, these rights will not be absolute; data controllers will be required to perform a 'balancing act' against any competing rights to freedom of expression when considering removal requests.

What is the current law?

The current Directive requires Member States to guarantee every data subject the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. Several Member States have construed this right narrowly in data protection laws implementing the Directive. For example, in the UK, the right for data subjects to apply to court for an order to rectify, block or destroy data is limited solely to where the court is satisfied that the data is inaccurate. As noted by the CJEU in the recent decision in Google Spain v AEPD and Costeja Gonzalez, the current Directive wording is much broader and the reference to the erasure right arising where data is incomplete or inaccurate is just a non-exhaustive example of where processing of personal data does not comply with the Directive.

What will change under the Regulation?

The 'right to be forgotten' is expressed in Article 17 of the Commission's draft of the Regulation as a "right to obtain from the data controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child", where one of four grounds applies. These include where the data are "no longer necessary in relation to the purposes for which they were collected or otherwise processed", where the data subject has withdrawn consent to processing, and where the data subject objects to the processing. Under the Commission draft, erasure must be carried out "without delay", subject to limited carve outs which include freedom of expression. As an alternative to erasure, it is proposed that the controller may instead restrict processing in certain limited circumstances. It is important to note that Article 17 requires controllers to weigh subjects' rights against any competing rights and interests including "the public interest in the availability of the data" when considering such requests. Whilst this will be applauded by exponents of freedom of speech, it nevertheless imposes a potentially onerous obligation upon otherwise neutral secondary controllers.

There appears to be general consensus between all three institutions that the 'right to be forgotten' should be a central part of the Regulation and that search engines in particular should fall within its scope. However the extent to which such controllers should be burdened with the responsibility for the removal of content remains a subject of disagreement. The Commission has proposed a requirement upon controllers to "inform third parties which are processing such data, that a data subject requests them to erase (...) personal data" (Article 17(2)), which will enable third parties such as publishers to have something of a say when removal requests are submitted to search engines in respect of their content. In contrast the EP's amended text goes even further than this, suggesting that the data controller "shall take all reasonable steps to have the data erased, including by third parties".

On either view, this means that many data controllers will be tasked with the role of judge and jury when considering such requests. The EP's proposal would also require secondary controllers to seek the removal of the content processed elsewhere by third-parties. The Council has yet to adopt a common position on Article 17 but the right to be forgotten has been the subject of much discussion at Council level,
10. The Right to be Forgotten (Article 17)

particularly in the light of the CJEU's decision in Google Spain. A note from the Presidency of 29 September reports that analysis, including the conclusion that that this right will be exercisable against all data controllers regardless of whether they obtained the data directly from the data subject or from secondary sources – essentially creating a new breed of intermediary obligations upon "secondary" controllers such as search engines, started by the CJEU in Google Spain.

Comment and practical advice

Whilst at present the internet community and Google have been quick to point out that the Google Spain decision only applies to search engines, it may only be a matter of time before the concept of a "right to be forgotten" or "right to erasure" is applied far more widely under the proposed Regulation. For the time being, the practical advice for controllers is to monitor the ongoing debate surrounding the implementation of the Google Spain decision and where the Council will land on the current drafting of the broader right to be forgotten in the draft Regulation. On 26 November 2014, the influential Article 29 Working Party issued a press release announcing the agreement and publication of criteria and guidelines to be followed by local data protection authorities and Member State law implementing the Google Spain decision.
11. International Transfers (Articles 40-45)

While the new regime builds on the current framework with respect to the general principles for international transfers, it is worth noting that the rules have been extended to apply to processors and to onward transfers of personal data to third countries or international organisations.

What is the current law?

Even in the borderless world of cloud computing and big data, the EU works as a protective cocoon when dealing with EU citizens' personal data. Indeed, in principle personal data transfers outside the EEA are only authorised to countries ensuring an "adequate" level of protection. The list of countries recognised as "adequate" is currently limited, so companies usually have to rely on other grounds to transfer data outside the EEA such as consent, necessity for the performance of an agreement or other adequate safeguards which include standard contractual clauses issued by the EU Commission and intra-group Binding Corporate Rules (BCRs). Some of the grounds for transfer, such as the US Safe Harbor, are now under attack (see for example the recent High Court of Ireland decision to refer the Schrems case to the European Court of Justice).

What will change under the Regulation?

The new framework for transfers, set out in Chapter V of the draft Regulation, still relies on adequacy decisions, appropriate safeguards and, in their absence, on derogations for specific situations. There is broad consensus between the institutions on the main features of the new data transfer regime. Key elements of the new regime include the following:

- **Adequacy decisions (the White List):** The three EU institutions intend to give exclusive competence over establishing the White List of adequate countries to the Commission (not to controllers, as argued by some Member States) and to list the assessment criteria within the Regulation. The EP and Council's texts ask the Commission to monitor decisions taken. The Commission may decide that a third country no longer ensures an adequate level of protection and may repeal, amend, or suspend an adequacy decision without retrospective effect. The EP and Council underline the need to obtain the European Data Protection Board's opinion on the assessment of the adequacy level.

- **Appropriate safeguards:**
  
  (i) Approved codes of conduct, approved certification mechanisms and instruments specific to the public sector have been added by the Council to the Commission's original list of appropriate safeguards on the basis of which a transfer can take place. The Council endorses the idea of a "European Data Protection Seal", introduced by the EP's suggested amendment, but the Council's proposed certification mechanism is broader.

  (ii) A distinction has been made between the appropriate safeguards which do not require a specific authorisation from a DPA (i.e. a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules (BCRs), standard clauses and approved codes of conduct and certification mechanisms with binding and enforceable commitments of the controller, processor or recipient in the third country) and those that remain subject to the authorisation of the competent DPA (e.g. ad-hoc contractual clauses).
(iii) BCRs remain widely-supported by all three institutions (with the addition of a full article on the mechanism) and may be extended to a “group of enterprises engaged in a joint economic activity” if the latest position agreed upon by the Council is supported.

- **Derogations to the prohibition on transfers:** The Council has added that, in order to be a valid ground for transfer, consent must be “explicit” while the Commission and the Parliament allowed mere consent to be a valid ground. The “legitimate interests” of the data controller has been added by the Commission as a valid transfer ground for transfers that cannot be qualified as “frequent or massive”. The EP has not taken this proposed new data transfer ground on board, while the Council accepts this ground when transfers are not large-scale or frequent and when such interests are not overridden by the interests or rights and freedoms of the data subject.

- **New additional limits to transfers:** The Council has added a new provision which may allow public authorities to limit transfers of specific categories of personal data on the basis of EU or Member State law for important reasons of public interest (e.g. electronic patient files) in the absence of a Commission adequacy finding and with an obligation to notify national measures adopted in this respect to the Commission.

**Comment and practical advice**

It is expected that the new transfer regime will carry forward most of the data transfer solutions available under the current framework with some further clarifications and a wide support for BCRs, codes of conducts and seals. Organisations need to be aware of the available data transfer solutions, even if they consider themselves to be a mere data processor, as the new regime (and fines for breaching the international transfer rules) will become applicable to processors. Data controllers should be aware of the risk that, if the EP's stricter position is adopted, their current data transfers based upon a country adequacy finding or on standard contractual clauses would only remain in force for five years after the entry into force of the Regulation, unless amended, replaced or repealed by the Commission before the end of this period. Similarly, current data transfers based on an authorisation by a supervisory authority would only remain valid for two years after the entry into force of the Regulation unless amended, replaced or repealed by the Commission before the end of this period.
Controllers must implement appropriate technical and organisational measures and procedures to ensure that processing safeguards the rights of the data subject (by design) and that, by default, only the minimum and necessary personal data for each specific purpose is processed and it is not disclosed more widely than necessary.

What is the current law?

The current Directive has no equivalent to the concept of privacy by design. However, during the three years that have passed since publication of the draft Regulation there has been much discussion and many ideas have been put forward to try to give the concept greater certainty and make its implementation workable and effective. For example, the principle has recently been developed in the context of smart metering in this Commission Recommendation on privacy impact assessments for smart grid and smart metering systems, which states that Member States should support data controllers in developing and adopting data protection by design and default solutions. The concept has also been explored in relation to the Internet of Things (IoT) in this recent Opinion by the Article 29 Working Party. The Opinion has stressed the importance of data protection by design and by default at all levels of the IoT value chain, in particular for device manufacturers, application developers and social platforms.

What will change under the Regulation?

All three institutions have a different stance on the issue. The debate has mainly been focused on the scope and details of the design obligations. While the Commission’s draft was less precise, the EP’s proposed text details the obligation to a greater extent, elaborating upon the benchmark that controllers should take into account when implementing technical and organisational measures. In addition to the state of the art, under the EP’s text, controllers must have regard to “current technical knowledge, international best practices and the risks represented by the data processing”, “the entire lifecycle management of personal data” and the results of the impact assessment, if any, proposing to remove the limit of the “cost of implementation” and most importantly, also extending the obligation to data processors. Furthermore, the EP has added privacy by design as a prerequisite for public procurement, in particular for utilities.

The latest draft of the Article, as amended by the Council, goes back to the Council’s initial version, but includes pseudonymisation of personal data as one of the technical and organisational measures to consider in privacy by design. In addition, the Council proposes certification mechanisms as a way of demonstrating controllers’ compliance, going a step further than the Commission (which merely stated in the last paragraph of the provision that it may set out technical standards for the privacy by design and by default requirements).

Comment and practical advice

Privacy and security should be taken into account by stakeholders not only at the final stages of the product or service configuration, but from its very inception. Privacy and security have to be embedded, by default and design, from the very outset. If the wording of the Regulation stays as it is in the latest Council draft, the cost of implementation will play a key role when assessing compliance with these obligations.
Key contacts

Blanca Escribano
Partner, Madrid
+34 91 187 1924
blanca.escribano@olswang.com

Sofia Fontanals
Senior Associate, Madrid
+34 91 187 1932
sofia.fontanals@olswang.com

Jack Gilbert
Associate, London
+44 20 7067 3817
jack.gilbert@olswang.com

Clive Gringras
Partner, London
+44 20 7067 3189
clive.gringras@olswang.com

Ashley Hurst
Partner, London
+44 20 7067 3486
ashley.hurst@olswang.com

Sofia Fontanals
Senior Associate, Madrid
+34 91 187 1932
sofia.fontanals@olswang.com

Jack Gilbert
Associate, London
+44 20 7067 3817
jack.gilbert@olswang.com

Clive Gringras
Partner, London
+44 20 7067 3189
clive.gringras@olswang.com

Thibault Soyer
Avocat à la Cour, Paris
+33 1 70 91 87 75
thibault.soyer@olswang.com

Christian Leuthner
Associate, Munich
+49 89 206 028-414
christian.leuthner@olswang.com

Ross McKean
Partner, London
+44 20 7067 3378
ross.mckean@olswang.com

Sylvie Rousseau
Partner, Paris/Brussels
+32 2 641 1272 / +33 1 7091 8787
sylvie.rousseau@olswang.com

Andreas Splittgerber
Partner, Munich
+49 89 206028-404
andreas.splittgerber@olswang.com

Matthias Vierstraete
Advocaat, Brussels
+32 2 235 0301
matthias.vierstraete@olswang.com

Claire Walker
Head of Commercial Group Know How, London
+44 20 7067 3174
claire.walker@olswang.com