An overview of the EU General Data Protection Regulation (‘GDPR’) for media organisations

The GDPR is a sweeping set of EU rules regulating the processing of personal data. It comes into force on 25 May 2018 in all member states of the EU. It has extra-territorial scope for data controllers outside the EU in certain circumstances and gives rise to litigation risks and tough enforcement measures in case of breach, including fines of up to 4% of annual global turnover or 20 million Euros. This note gives a general overview of the GDPR and how it may potentially impact media and other organisations, including the conflict between the rights of data subjects and the right of free speech.

Contents

What is the GDPR? 2
Brexit 3
Territorial Scope of the GDPR? 3
What will data controllers have to do under the GDPR? 4
Obligations on data controllers 5
Principles 6
Rights of Data Subjects 7
Data processors 8
Exemptions 9
The journalistic exemption 9
What legal and regulatory risks arise for organisations in breach of the GDPR? 12
Regulatory framework 13
Regulatory powers 13
Fines 14
Civil litigation risks 15
Enforcement across borders on non-EU media organisations 16
What is the GDPR?

The GDPR is a comprehensive European Union regulation overhauling the current EU data protection regime. The overarching purpose of the law is to provide enhanced protections for individuals, to create more control over data processing operations and improve trust and confidence in security and privacy protection in the face of modern technology and globalisation. The GDPR considerably strengthens data subject rights, the obligations on those processing personal data and the sanctions that can be imposed against those who fail to comply.

The GDPR will supersede the EU Data Protection Directive 95/46/EC (the “Directive”), and impose new rules and obligations on those who process “personal data” and/or “special categories of personal data” as defined below.

- “Personal data” is any information about any living, identified or identifiable person (defined as the “data subject”). This is a broader definition than the current law. It not only includes a person who can be identified, directly or indirectly, by reference to factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, but also by reference to identification numbers, location data or online identifiers. These could be generated by a data subject’s devices or Apps, for example, an IP address, cookie identifiers or browsing history, which can be used to profile data subjects.

- “Special categories of personal data” (Article 9 of the GDPR) refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person’s sex life or sexual orientation. This is broadly equivalent to the term “sensitive personal data” under the Directive. However, data relating to criminal convictions or offences is no longer included in the special category definition and is dealt with separately under Article 10 of the GDPR. It will be for EU Member States themselves to provide appropriate, additional safeguards for data subjects by implementing national rules. The UK Government has stated an intention to do this via new legislation to “ensure that the data of victims, witnesses and suspects of crimes, are protected in the context of criminal investigations and law enforcement action”.

The definition of “processing” is broadly similar to that in the Directive and covers almost any operation, automated or not, performed on personal data or sets of personal data. It not only includes actions such as collecting, organising, altering, transmitting or destruction, but also storing data. This will cover not only the processing of customer data but also media and social media content referring to identifiable individuals.

The GDPR will become the law on 25 May 2018 with direct effect in all EU Member States. This means that it will become immediately without the need for further action from national EU governments, except where the GDPR leaves gaps for Member States to implement national rules.

The GDPR will directly impose specific obligations on:

- “controllers”, an individual or entity which alone or jointly with others, determines the purposes and means of the processing of personal data; and

- (for the first time) “processors”, an individual or entity which processes data on behalf of the controller.

Its effects are expected to be transformative for businesses. There will be no grace period.

---

Brexit

As the UK will still be part of the EU on 25 May 2018, the GDPR will become law in the UK on that date. Any inconsistent parts of the Data Protection Act 1998 (‘DPA’) (the existing law which implements the Directive in the UK) will be repealed.

After Britain has left the EU (‘Brexit’), perhaps at the end of March 2019 or later, the UK may no longer be subject to EU law or decisions of EU courts. The UK Government has stated that it does not envisage much change to UK data protection law as a result of Brexit. Providing fewer rights than the GDPR on Brexit could jeopardize UK/EU trade and data flows. However, Brexit will create potential problems and uncertainties regarding, for example, data flows with the EU, the application of EU judgments, what happens when there are amendments to the GDPR as well as if and how the UK data protection regulator co-operates with other EU regulators. These areas will need resolving.

Territorial Scope of the GDPR?

The GDPR’s territorial reach will expressly stretch beyond the EU (the ‘Union’) for the first time. Article 3 states:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   b. the monitoring of their behaviour as far as their behaviour takes place within the Union.

Article 3 builds on the principle established in the Court of Justice of the European Union decisions in the Google Spain and Weltimo cases that companies not processing data within the Union can still be subject to EU data protection law, provided the processing takes place in the context of the activities of a controller or a processor established in the Union. In Google Spain, Google Inc. was held to be a data controller and subject to EU data protection law because its activities were inextricably linked to the activities of a Spanish subsidiary established in a Member State so as to make the parent company economically profitable. In Weltimo, the court stated that the concept of establishment “extends to any real and effective activity – even a minimal one – exercised through stable arrangements” in a Member State.

Article 3(2) goes further by expressly linking the application of the GDPR to the processing activities of a controller or data processor established outside of the EU which offer goods and services to data subjects in the EU or monitor their behaviour in the EU. Recital 23 to the GDPR indicates that offering goods and services occurs where it is apparent that a controller is envisaging offering goods and services in an EU Member State. A website’s mere accessibility from within the EU or being written in an EU language or having EU contact details will not be determinative per se. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or references to customers or users in the Union, may make it apparent that the controller envisages offering goods and services to data subjects in the EU. Monitoring behaviour relates to tracking individuals on the internet, such as profiling users in order to take decisions about them or for analysing or predicting personal preferences, behaviours and attitudes. For example, if a non-EU media organisation runs a website funded by online behavioural advertising that profiles EU citizen’s web browsing history and IP addresses in order to deliver meaningful and relevant adverts upon each visit, that organisation would likely be caught by the GDPR.
In these ways, the law’s focus will shift away from a data controller’s or server’s geographical location and where the processing takes place, towards the type of processing that it carries out, the location of the data subjects and/or where the controller’s subsidiaries are established. This extra-territorial reach will be significant for many non-EU media organisations which will, as a result, be categorised as controllers, becoming exposed to the full force of the GDPR or, to a lesser extent, as data processors (see more below). The broadening of the scope for EU established controllers and processors and for specific activities of non-established entities to which the law applies will also potentially expose such entities to the enhanced sanctions and potential civil litigation for non-compliance.

Where Article 3(2) applies, the controller or processor must designate a representative in the EU unless the processing is occasional, does not include on a large scale the processing of special categories of data or data relating to criminal offences and is unlikely to result in a risk to the rights and freedoms of individuals. The representative should act on behalf of the controller or processor with regard to their obligations under the GDPR and be addressed by any supervisory authorities. According to Recital 80, “the designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor”. Whilst controllers and processors remain liable, it appears that enforcement action could be taken by representatives instead or as well. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

What will data controllers have to do under the GDPR?

Organisations impacted by the GDPR will have to abide by a new level of regulatory compliance (or face penalties for non-compliance) and, subject to exceptions, will have to comply with requests from data subjects who seek to enforce their rights (or face complaints to regulators or civil litigation through the courts).

There will be a disparity in effect between data controllers and processors. Data controllers will have to comply with all the provisions of the GDPR. Data processors will have to comply to a lesser extent. Anyone processing personal data will need to consider which category they fall into as the obligations, requirements and rights compliance duties differ.
Obligations on data controllers

The following key obligations (see Articles 24-50 for full details) will, subject to a Member States’ discretion to enact national provisions imposing further detailed rules or derogations (where permitted under the GDPR), affect data controllers:

1. To **comply with the data protection principles** (see below).

2. To **facilitate the exercise of the rights of data subjects** (see below).

3. To **keep records** of data processing activities.

4. To appoint a **data protection officer** where an organisation’s core business involves processing personal data involving regular and systematic monitoring of data subjects or large amounts of sensitive personal data.

5. To **report data breaches** to the relevant regulator without undue delay and, where feasible, within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. **Data subjects must be informed** without undue delay where a breach is likely to result in a high risk to the data subject’s rights and freedoms unless the data has been rendered unintelligible (for example by encryption), the data controller has taken steps to ensure the high risk is unlikely to materialise or it would involve disproportionate effort to inform data subjects individually (in which case a public announcement can be made).

6. When relying on consent to process personal data, data controllers will need to show that the **consent is freely given, specific and informed and is an “unambiguous indication” of a data subject’s wishes and expressed either by a statement or a clear affirmative action. Explicit consent is required for processing special categories of data**.

7. Controllers will be required to carry out **data protection impact assessments** if their proposed activities are likely to result in a high risk to the rights and freedoms of individuals, in particular through the use of new technologies or people profiling. A data controller must consult the competent “Data Protection Authority” prior to starting the processing when the impact assessment indicates that such processing is likely to result in a high risk to individuals in the absence of measures taken by the data controller to mitigate such risk.

8. **Privacy by design and default.** Controllers must, taking into account factors such as the state of the art (i.e. new technologies) and costs, build into systems and processes by default appropriate technical and organisational measures for the protection of data subjects and GDPR compliance.

9. Restrictions on **transfers/exports of personal data outside the EU** whereby transfers can be made under a Commission adequacy decision (a statement published by the Commission, one of the governing bodies of the EU) or if standard contractual clauses or Binding Corporate Rules (‘BCRs’) for intra-group transfers are in place. These provisions are broadly similar with formal recognition for BCRs and media organisations will be aware of the current ‘Privacy Shield’, which allows transfers of personal data from the European Union to US organisations which voluntarily certify under the Privacy Shield framework (see further information on our website: www.taylorwessing.com/en/news/the-eu-us-privacy-shield-getting-your-certification-ready

10. The default age where parental consent is required for a **valid, digital consent for** processing the personal data of **minors** using online services is set at under 16, but Member States can reduce this threshold to as low as under 13.

Registration as a data controller is no longer required but is replaced by the obligation to maintain internal records of processing. Conditions for lawfully processing data are located in Articles 6 and 9 of the GDPR respectively.
Principles

Article 5 of the GDPR sets out 6 principles which data controllers (not processors) shall be responsible for complying with and demonstrating their compliance with when processing data. Personal data shall be:

1. processed **lawfully, fairly and in a transparent** manner in relation to the data subject;
2. collected for specified, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, i.e. **data minimisation**;
4. **accurate** and, where necessary, kept up to date and every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, is erased or rectified without delay;
5. kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed; and
6. processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, the controller shall be responsible for, and be able to demonstrate, their **compliance** with the above principles.

The rules on lawful processing of personal data and special categories of personal data are set out in Articles 6-11. In the case of personal data (rather than special categories of personal data), processing is lawful if and to the extent there has been relevant consent or, for example, where the processing is necessary:

- for the performance of a contract to which the data subject is a party; or
- for compliance with a legal obligation to which the controller is subject; or
- to protect the vital interests of the data subject; or
- for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.
Rights of Data Subjects

Under Articles 12 – 22 of the GDPR, data subjects will have new and enhanced rights to help them control the use of their data, with which data controllers need to comply, as follows.

1. The right to be informed – information must be provided to data subjects about the processing, categories and sources of their data so that processing is fair and transparent. The GDPR sets out the specific information that must be provided to data subjects.

2. The right of access – data subjects have the right to obtain confirmation about whether a controller is processing their data and are entitled to access to a copy of that data and supplemental information, such as the purpose of processing, categories, recipients, retention periods and sources of data.

3. The right to rectification – data subjects can require a controller, without undue delay, to rectify inaccuracies in personal data held about them or to complete incomplete data.

4. The right to erasure (“right to be forgotten”) – this requires data controllers, without undue delay, to erase data where its processing fails to comply with the GDPR, for example if:
   a. the data is no longer necessary for the purposes it was collected for;
   b. consent is withdrawn and no other legal justification for processing exists;
   c. the data subject objects and there are no overriding legitimate grounds for processing;
   d. data has been processed unlawfully; and/or
   e. the data must be erased to comply with the law.

In addition, where a data controller has made the personal data public and has to erase it, it must take all reasonable steps (taking into account technology and costs) to inform other controllers which are processing the data that the data subject has requested the erasure of any links to, or copies or replications of, that data.

The right to erasure shall not apply to the extent that the processing is necessary e.g. for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of tasks carried out in the public interest or for certain archiving purposes or for the establishment, exercise or defence of legal claims.

5. The right to restrict processing – requires data controllers to mark data and not process it beyond simply storing it (unless the data subject consents or processing is necessary for establishing, exercising or defending legal claims, protecting others’ rights or for an important public interest of the EU or a Member State) where:
   a. data accuracy is disputed and time is required to verify the accuracy;
   b. a data subject has objected to processing and requires this restriction pending verification of whether the legitimate grounds of the controller override the rights of the data subject;
   c. where processing is unlawful, but the data subject requests a restriction on use of the data rather than erasure; and/or;
   d. when a controller no longer needs the data, but the data subject requires it to establish, exercise or defend a legal claim.
6. The right to object to:
   a. processing (necessary for the purposes of the legitimate interests pursued) by the data controller, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or processing is for the establishment, exercise or defence of legal claims; and (separately)
   b. personal data processed for direct marketing purposes (including profiling) at any time, after which the personal data shall no longer be processed for such purposes.

7. The right to data portability – the right to receive one’s personal data, which the data subject has provided to the data controller, in a structured, commonly used and machine-readable format and the right to transmit that data to another controller without hindrance from the previous controller, as long as processing is carried out by automated means and based on (i) consent or (ii) a contract to which the data subject is a party. This could potentially give a person the right to transfer their profile or content to another media company or internet service provider.

8. Rights not to be subject to automated decision making and profiling which has a legal or other significant effect on the data subject, subject to exceptions.

Data processors

Data processors are also now directly bound by a subset of provisions under the GDPR (mainly Articles 28-37), albeit a lighter set than those for data controllers. The key obligations are as follows.

1. Processors are under an obligation to comply with controllers’ instructions and maintain a record of all categories of processing activities and a record of the processing activities carried out on behalf of a controller, including categories of processing set out in the GDPR (Article 30(2)).

2. Processors are required to appoint a data protection officer in certain situations, including where the data processing activities require regular monitoring of data subjects on a large scale, or where the core activities of the processing involve large amounts of special (sensitive) data or data relating to criminal convictions and offences.

3. Data processor activities must be governed by a binding contract with regard to the controller. The data processor has an obligation to tell the controller if it believes that an instruction to hand information to the data controller breaches the GDPR or any other EU or individual Member State’s law.

4. Processors, like controllers, are required to implement appropriate security measures.

5. Processors are required to notify their relevant controller of any breach without undue delay after becoming aware of it.

6. The processor has to exercise a degree of independence from the controller when deciding whether or not it can transfer personal data to a country outside of the EU.

Processors may also be obliged to support data controllers in the performance of their obligations under the GDPR.
Exemptions

There are exemptions under the GDPR allowing controllers and processors to derogate from the specific personal data processing provisions and are found in Articles 85-91 of the GDPR. They include certain processing relevant to:

- Freedom of expression and information
- Public access to official documents
- National identification numbers
- Employee data
- Scientific and historical research purposes or statistical purposes
- Archiving in the public interest
- Obligations of secrecy
- Churches and religious associations.

In these areas there is potential for disparity between different EU Member States, as each will have the ability to introduce supplemental laws or derogations relevant to these special situations as well as derogations on issues such as national security, public security, the protection of judicial independence and proceedings and the enforcement of civil law matters, subject to these national measures being necessary and proportionate.

The journalistic exemption

Of key relevance to media organisations is the exemption relating to freedom of expression and information under Article 85, which states: “Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression”. Recital 153 of the GDPR includes that “In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.”

The journalistic purposes derogation, where relevant, applies to most of the provisions of the GDPR (including the principles, the rights of data subjects and transfers of personal data to countries outside of the EU) meaning that the processing subject to it will generally not have to be compliant with those parts of the rules. National Governments will be required to put legislative measures in place to implement this exemption, which shall be enforced by local regulatory authorities. In the UK, this will be the Information Commissioner’s Office (the ‘ICO’).
In the UK, the DPA currently contains the special purposes exemption under section 32 (the ‘journalistic exemption’) which exempts data controllers from complying with most of the provisions of the DPA and states:

1. Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if —
   a. the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
   b. the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
   c. the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

Although section 32 of the DPA is likely to be repealed, the UK Government, via the Department for Digital, Culture Media & Sport, published on 7 August 2017 a statement of intent entitled “A New Data Protection Bill: Our Planned Reforms” confirming that a new provision, but one broadly replicating the existing section 32 (which it states strikes “the right balance”) will be enacted in its place when the GDPR comes into force. The main difference will be to amend provisions relating to the ICO’s enforcement powers to strengthen its ability to enforce the re-enacted journalistic exemption effectively. On 14 September 2017 the Government published the Data Protection Bill which is intended to replace and repeal the DPA and to deal with various matters reserved to EU Member States by the GDPR, including Article 85.

Part 5 of Schedule 2 of the Bill states, at paragraph 24 (which follows section 32 of the DPA), that:

1. In this paragraph, “the special purposes” means one or more of the following—
   a. the purposes of journalism;
   b. academic purposes;
   c. artistic purposes;
   d. literary purposes.

2. The listed GDPR provisions do not apply to personal data that is being processed only for the special purposes to the extent that—
   a. the personal data is being processed with a view to the publication by a person of journalistic, academic, artistic or literary material,
   b. the controller reasonably believes that publication of the material would be in the public interest; and
   c. the controller reasonably believes that the application of any one or more of the listed GDPR provisions would be incompatible with the special purposes.

3. In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

4. In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (5) that is relevant to the publication in question.

5. The codes of practice and guidelines are—
   a. BBC Editorial Guidelines;
   b. Ofcom Broadcasting Code;
   c. IPSO Editors’ Code of Practice". 
With reference to sections 32(4) and 32(5) of the DPA, section 166 of the Bill deals with staying special purposes proceedings and states:

1. In any special purposes proceedings before a court or tribunal, if the controller or processor claims, or it appears to the court or tribunal, that any personal data to which the proceedings relate –
   a. is being processed only for the special purposes,
   b. is being processed with a view to the publication by any person of journalistic, academic, literary or artistic material, and
   c. has not previously been published by the controller, the court or tribunal must stay the proceedings.

2. In considering, for the purposes of subsection (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

3. Under subsection (1), the court or tribunal must stay the proceedings until either of the following conditions is met—
   a. a determination of the Commissioner under section 164 with respect to the personal data or the processing takes effect;
   b. where the proceedings were stayed on the making of a claim, the claim is withdrawn.

The following decisions in the English civil courts on the interpretation of section 32 give an indication of how things will likely continue after the GDPR comes into force in England.

- **Steinmetz v Global Witness [2014] EWHC 1186 (Ch)** – The ICO (having been referred this issue by the English High Court) decided that section 32 applied broadly to anyone engaged in public interest reporting, not just conventional media organisations, and that journalism is widely defined as imparting information, opinions and ideas for general public consumption. This allowed Global Witness (a not for profit NGO which raises public awareness and campaigns on alleged corruption relating to natural resources) to defend the claims being brought against it under the DPA. Further, the ICO stated that its role was not to decide if there was a public interest, but whether the data controller’s belief that there was one was reasonable.

- **Stunt v Associated Newspapers [2017] EWHC 695 (QB)** – The English High Court held that section 32(4) of the DPA, which effectively stays a civil data protection claim brought against a data controller in respect of unpublished data held for the purposes of journalism was not incompatible with EU law. The court ordered that the relevant parts of the data protection claims brought against the defendant publisher (for alleged failure to comply with subject access, erasure and cease processing requests) be stayed under section 32(4).

Along with these cases, other indications of how the ICO might deal with section 32 issues if empowered by a new, similar provision pursuant to Article 85 of the GDPR, come from the ICO’s guidance entitled “Data protection and journalism: a guide for the media”. This recommends, for example, that media organisations have clear policies on what content requires editorial approval, provide awareness training to staff on data protection, create an inbuilt public interest check at key stages of a story (e.g. when using covert methods or giving a final decision to publish) and keep an audit trail for high-profile or intrusive stories.
What legal and regulatory risks arise for organisations in breach of the GDPR?

If a breach occurs, an organisation will be exposed to regulatory intervention, complaints to regulators and fines as well as civil litigation brought by aggrieved data subjects against regulatory decisions or directly against controllers/processors, plus claims for compensation.

The big difference between the GDPR and the current law (see below) comes from the scope of regulatory powers and the size of fines available as well as the enhanced and additional legal and regulatory rights given to data subjects (either individually or via class actions). The number of potential offenders/targets will also increase because of the GDPR’s expanded scope, including its world-wide territorial reach.
Regulatory framework

Data controllers will be regulated by a lead Supervisory Authority (‘LSA’) in the place of their main establishment which will be the main administrative location in the EU unless the main decisions about data processing are taken in a different Member State, in which case that will be the main establishment. This changes the current position where entities that operate in different Members States are subject to the jurisdiction of the relevant authority in each Member State. Controllers without any establishment in the EU must deal with the local supervisory authority in every Member State in which they are active, through their local representative. In addition:

- Individuals will be able to make complaints in their own Member State at which point that regulator will investigate, subject to its engagement in a cooperation procedure with the LSA (which can intervene).
- Data protection regulators in other Member States (rather than LSAs) will also be able to deal with any breaches arising in their own jurisdictions or issues which substantially affect only data subjects located within it. They shall also be able to deal with individuals’ complaints made in their Member State, again subject to engaging in a cooperation procedure between the regulators and the LSA.

Mutual assistance and joint investigation provisions exist under the GDPR to ensure that authorities in different Member States help each other and work together and endeavour to reach a consensus on their decisions. Regulators from other Member States, other than the LSA, will have the right to be involved in enforcement operations if a controller has an establishment in its territory or a significant number of its data subjects are likely to be affected. Any disagreement will be settled by the independent European Data Protection Board (EDPB). In relation to such disputes (which may typically be expected to arise between an LSA and another regulator) the EDPB will issue a binding verdict on the basis of a two-thirds majority vote.

Regulatory powers

Supervisory authorities, either through their own regulatory initiatives or when dealing with complaints made by data subjects, will have various powers of intervention, including investigative and corrective powers, as well as the ability to levy large fines up to a maximum of 20 million Euros or up to 4% of total worldwide turnover of the preceding financial year, whichever is higher.

Their investigative powers include information disclosure orders, data audits, breach notifications and access to data being processed, premises and equipment.

Their corrective powers include fines, infringement warnings, issuing reprimands, compliance orders and orders compelling or imposing:

- the controller to communicate a personal data breach to the data subject;
- temporary or definitive limitations, including a ban on processing;
- the rectification, restriction or erasure of data; and/or
- the suspension of data flows to a recipient in a country outside of the EU.
Fines

As mentioned above, fines substantially increase under the GDPR from previous thresholds. Higher tier fines can be up to 20 million Euros or 4% of annual global turnover and lower tier fines can be up to 10 million Euros or 2% of annual global turnover (whichever is the greater in either case).

Although dependent on the circumstances of each case, typically penalties will only be imposed in addition to or instead of the LSAs’ corrective powers. When deciding whether or not to administer a fine, the following circumstances will be considered:

- The nature, gravity, and duration of the infringement (also with regard to the purpose of the processing, the number of data subjects affected and level of damage suffered by them);
- Whether the infringement was intentional or negligent;
- Any action taken by the data controller or data processor to mitigate the damage suffered by data subjects;
- The degree of responsibility of the data controller or data processor with regard to technical and organisational measures implemented by them;
- Any previous infringements by the controller or processor;
- The degree of cooperation with the LSA in order to remedy the infringement and mitigate any adverse effects;
- The categories of data affected by the infringement;
- The manner in which the infringement becomes known to the LSA;
- Any previous imposition of corrective powers on the controller or processor;
- Adherence to approved codes of conduct or approved certification mechanisms; and
- Any other aggravating or mitigating factor such as financial benefits gained or losses avoided either directly or indirectly from the infringement.

Some breaches will expose a data controller or processor to the higher potential penalty, whilst some breaches are capped at up to half of the full potential penalty. Below are some examples that may be relevant:

**Up to the full fine (20 million or 4%) for failure to:**

- process data lawfully and fairly, in a transparent manner, in a way compatible with the initial purpose and accurately;
- demonstrate that consent was given by the data subject to the processing where it is used as the basis for processing;
- process special categories of personal data within the applicable requirements;
- provide confirmation to the data subject as to whether their personal data is being processed and where, and access to it;
- rectify inaccurate personal data or erase it or provide restriction to it and communicate the same;
- provide to a data subject their data which has been provided to a controller in a structured, commonly used and machine readable format;
- comply with the rules for transferring data outside of the EU; or
- comply with an order or a temporary or definite limitation on processing or a suspension by an LSA pursuant to their powers.
Up to half of a full fine (10 million or 2%) for failure to:

- obtain parental consent verification in the case of processing personal data of a child;
- implement appropriate technical and organisational measures to ensure that data protection is enshrined by design and default and to ensure a level of security appropriate to the risk;
- designate a representative in the EU and a data protection officer and maintain a record of processing activities under its responsibility;
- use data processors providing sufficient guarantees to implement appropriate technical and organisational measures;
- process within the instructions of the data controller;
- notify the personal data breach to the competent LSA without undue delay and where feasible not later than 72 hours after having become aware of it and, where a data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay;
- carry out a data protection impact assessment prior to carrying out processing which is likely to be high risk to the rights and freedoms of individuals; or
- comply with LSA codes of conduct and certification requirements.

Civil litigation risks

In the same way that data controllers can be sued in England in relation to media content directly under the DPA by data subjects, they can also be sued for a breach of the GDPR by a data subject (or by many data subjects via a class action). Data subjects can also claim compensation for material or non-material damage (such as distress). As a result, Article 85 and whatever journalism exemptions are in place across Member States under the GDPRs will become the main battleground.

Data subjects also have a right to an effective judicial remedy against an LSA decision concerning them, or a failure by the LSA to deal with a complaint within 3 months.

The implementation of the GDPR is likely to spark litigation in the same way that the decision in Google Spain (where a US company was held to be subject to EU data protection law as a data controller) did. The express extra territorial scope of the GDPR will enshrine the possibility for EU data subjects to sue non-EU media organisations for breach. For example, the English Courts have been willing to allow UK data subjects to serve English proceedings outside of the jurisdiction on US data controllers:

- **Hegglin v Person(s) Unknown & Google Inc [2014] EWHC 3793 (QB)** – The English High Court allowed claims under the DPA, to cease processing and erase anonymously posted, highly defamatory and abusive allegations, to be served out of the jurisdiction on Google Inc., holding that there was a good, arguable case that Google Inc. was obliged to comply with the DPA when processing data as a web host, as well as when operating a search engine (following Google Spain).

- **Mosley v Google [2015] EWHC 59 (QB)** – After Max Mosley obtained court decisions in France and Germany whereby Google Inc. had to de-index and block access to images (rather than simply retrospectively remove URLs on request), the English court refused to strike out similar data protection claims brought under the DPA for erasure, cease processing and damages holding such claims as viable so that they should proceed to trial.
Vidal-Hall v Google Inc [2015] EWCA Civ 311 – This was a decision on a point of law establishing a claimant’s ability to claim damages for distress (without financial loss) for alleged breaches of data protection law. In this case, the allegation was that Google had been tracking and collecting Apple Safari users’ browser-generated information regarding their internet usage without their knowledge, which Google gave to advertisers. The advertisers then targeted the users with ads on their display screens which were seen by others causing distress to the users. The ability to claim compensation for distress is reflected in Article 82 of the GDPR which applies to data controllers’ and data processors’ liability for ‘non-material’ damage. The English court also recognised that a claim under the DPA would fall into one of the jurisdictional ‘gateways’ allowing a claimant to serve English court proceedings outside the jurisdiction on a US defendant.

The above cases settled before going to trial. However, these cases demonstrate the potential power of bringing data privacy disputes to a settlement instead of having a trial potentially establishing damaging legal precedents for either party. The expansion of rights under the GDPR will likely fuel further civil litigation and the development of the law in different Member States of the EU and via the CJEU.

The GDPR also creates additional potential liability issues as where more than one controller or processor, or both a controller and a processor, are involved in the processing and where they are responsible for any damage caused by processing, each controller or processor is jointly and severally liable for the entire damage in order to ensure effective compensation of the data subject. This could spark litigation between controllers and processors seeking to apportion liability, as controllers or processors can claim contributions against other such parties where they have paid full compensation (unless the party is exempt from liability because they are not in any way responsible for the event giving rise to the damage).

Enforcement across borders on non-EU media organisations

In the event of an EU data protection regulator imposing a corrective measure - for example, a 20 million Euros fine, or an EU national Court ordering a data controller to block or erase personal data along with payment of compensatory damages, - the question arises whether a non-EU data controller will need to comply and, if not, how the GDPR can be enforced.

In this global inter-connected world, it will be relatively unusual for a GDPR regulated non-EU controller not to have any assets in the EU against which a court order or fine could be enforced. Even if there are no EU assets on the date of the fine or court order, it may be that such a non-EU organisation could wish to set up operations in the EU in the future. Therefore, most non-EU organisations are, in practice, likely to need to comply even if enforcement in the their jurisdiction may not technically be possible. Ultimately, enforcement in their jurisdiction is a matter of local law.

The mechanism for non-EU enforcement is currently unclear. The GDPR is essentially an EU privacy statute for the 21st century but, in parallel, there is little evidence of an injunction granted by e.g. an English Court preventing the disclosure of private information (e.g. under the tort of misuse of private information) being enforceable in the US. For example, in the PJS v News Group Newspapers (Supreme Court, 2016) case, one of the reasons why the UK defendant publisher challenged the English interim injunction initially granted in that case was because the private information subject to the order had been published in other jurisdictions (including the USA). Non-EU publishers in a similar case from 25 May 2018 might potentially also be subject to the GDPR.

As mentioned above, under the GDPR, non-EU data controllers will generally be required to appoint an EU “representative” to represent the controller or processor. Enforcement action could potentially be brought against the representative (see above). Therefore, companies who are willing to be representatives may require indemnities from the controller and/or potentially seek insurance if they are to take on this role. Failing to adhere to appoint a representative is a breach in itself (see above). Failure to comply with the GDPR,
regulatory fines or court orders (particularly following a data breach) will also potentially cause reputational damage, especially as the GDPR is there for consumers to better protect their privacy. The GDPR could also affect insurance premiums for controllers, processors and representatives seeking to mitigate the new risks by taking out insurance.

To further understand the different data protection issues which will affect your and your clients’ global business operations and international data protection issues, including the GDPR and a world map of higher and lower risk data protection jurisdictions, please see the Global Data Hub on Taylor Wessing’s website: www.taylorwessing.com/globaldatahub/.

If you would like further information, please do not hesitate to contact us.

Timothy Pinto is a Senior Counsel and Michael Yates is an Associate specialising in media, data privacy and intellectual property law. Tim is head of Taylor Wessing UK’s publishing group. Sally Annereau is a Senior Advisor specialising in data protection and previously worked for six years at the UK Information Commissioner’s Office. They work in the London office of international law firm Taylor Wessing

2 October 2017