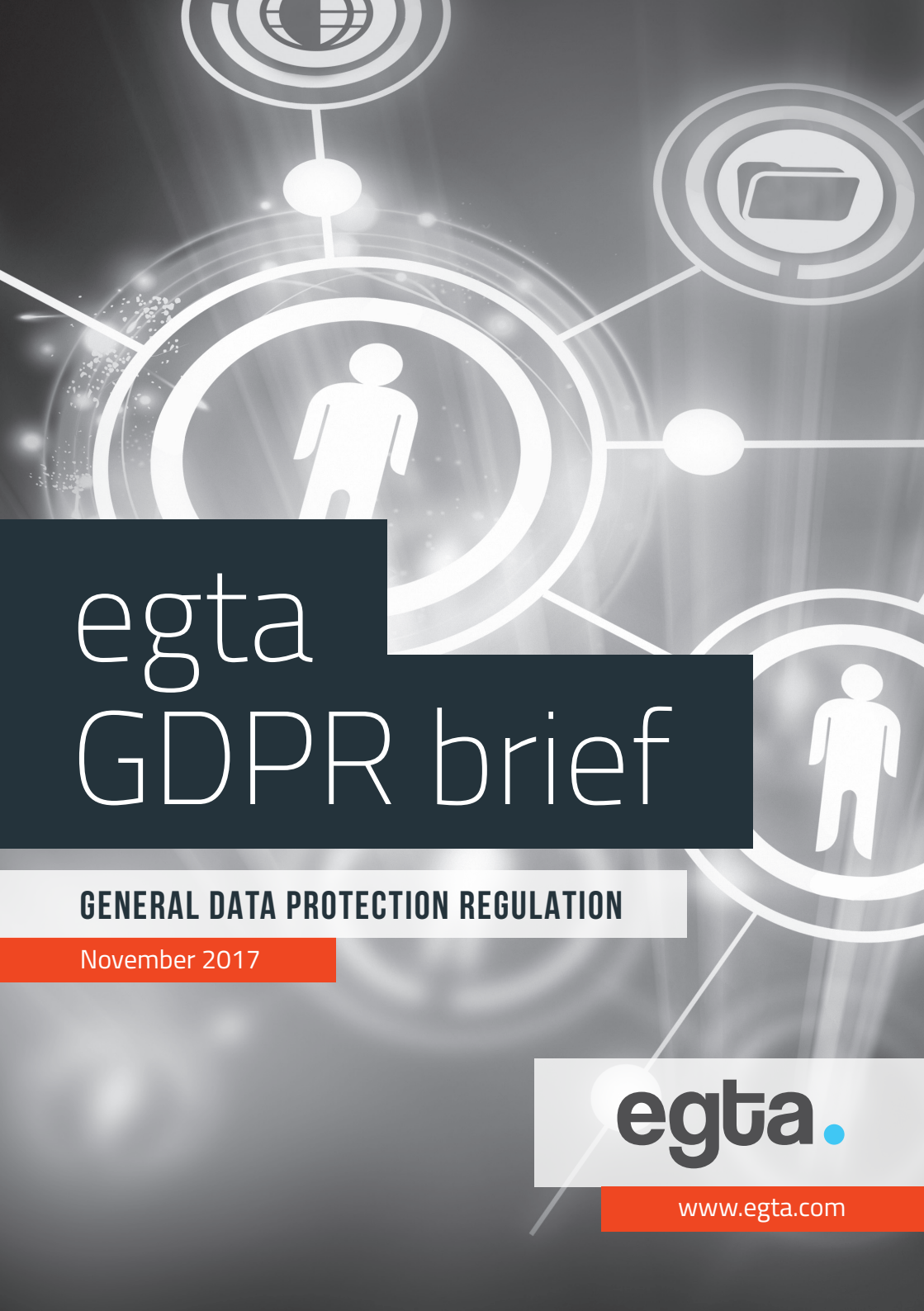


egta GDPR brief

GENERAL DATA PROTECTION REGULATION

November 2017

egta.

www.egta.com

WITH THANKS TO OUR PARTNER

This brief has been prepared with the active collaboration of Improve Digital, which offers an all-in-one advertising platform for publishers, content providers and broadcasters. Improve Digital works with over 250 of the world's top media owners, an audience of more than 600 million unique visitors and, through them, supports the efforts of 112,000 advertisers each month.

DISCLAIMER

The content of this publication is intended as a non-exhaustive overview of the potential impacts of the General Data Protection Regulation on egta members' activities and is neither provided as legal advice nor as a compliance tool.

Although our objective is to provide our members with the clearest and most accurate information, **egta and Improve Digital disclaim any liability in connection with the use of the information provided in this document.**

egta, Brussels, November 2017

TABLE OF CONTENTS

LEXICON

Article 29 Working Party: the Article 29 Working Party is an advisory body of representatives from National Data Protection Authorities of the EU member states.

CBR: Corporate Binding Rules

DPA: Data Protection Authority

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

ePR: ePrivacy Regulation

GDPR: General Data Protection Regulation

SCC: Standard Contract Clause

SSO: Single Sign-On system (centralised log-in system across several services)

INTRODUCTION:

The EU General Data Protection Regulation ('GDPR') will enter into force on 25th May 2018 in all EU Member States, replacing the current Data Protection Directive which dates back to 1995.

The GDPR builds on existing rules but introduces significant changes: therefore, any organisation processing personal data needs to carry out a thorough examination of its activities in order to ensure compliance with the new framework.

This requires important internal adjustments as well as coordination across the advertising value chain.

With only a few months to go, sales houses should already be quite advanced in their adoption process, not only because of the responsibility towards users and the risks in terms of brand image, but also because of the considerable economic sanctions that the GDPR introduces (up to 4% of a company's annual global turnover or €20 million, whichever is higher).

However, a survey carried out by egta among its members in May 2017 showed that less than 50% of CEOs interviewed had prepared for GDPR implementation.

This publication is designed for TV and radio sales houses, both as a reminder of the challenges and questions raised by the GDPR on their day-to-day activities and as a means of learning from the experience of other sales houses regarding the practical issues they have faced in preparing for this new piece of legislation.

> "We are in regular talks with advertisers, media agencies and other third parties who expect broadcasters and their sales houses to actively address the challenges related to GDPR implementation".
>
> **--- RTL Mediengruppe**

PART 01:

MATERIAL AND GEOGRAPHICAL SCOPE

The GDPR applies only to the processing of **personal data**, defined as "*any information relating to an identified or identifiable natural person*".

Identification may occur by associating online identifiers with other information to create profiles[1] and, to qualify as personal data, it is not necessary that all the information enabling the identification of the data subject be in the hand of one person[2]. Location data or online identifiers are clearly mentioned as types of data that may be used to identify users.

Pseudonymised data is no longer attributable to a specific data subject without the use of additional information, which should be kept separately and subject to technical and organisational measures. Pseudonymous data **is** considered personal data and is regulated under the GDPR; however it can be used to satisfy certain obligations[3].

Anonymous data is not considered personal data, and as such falls outside the scope of the GDPR. Anonymisation is meant for irreversible de-identification.

The **territorial scope** of the GDPR covers:

- The processing of personal data by controllers and processors established in the EU, regardless of whether this takes place in the Union or not;
- The processing of personal data by companies outside the EU where it relates to the offering of goods and services to data subjects in the EU (with or without payment) or to the monitoring of their behaviour taking place in the EU.

IN PRACTICE:

Personal data should be considered as an extensive concept: to the extent that it is **possible** (however difficult) to trace someone back through information, that information may qualify as personal data.

The **context** of data processing is important: for example, hashed identifiers[4] may not be considered personal data unless the controller/processor of the data can reasonably collect additional information to single out a user.

According to IAB Europe, "*under the GDPR, online identifiers and information related to those identifiers will often constitute personal data. (...)* ***The types of pseudonymous data commonly used by companies in the online advertising industry, such as device advertising identifiers and cookie IDs, will*** *(depending on the specific situation of the company processing the data)* ***generally fall into the category of personal data and thus be subject to the requirements of the GDPR***"[5].

As is currently the case, sensitive data (revealing political opinion, ethnicity, sexual orientation, etc.) remains subject to stricter conditions.

PART 02: BASIC PRINCIPLES

The GDPR presents the basic principles that any data processing operation should follow.

Main changes in comparison with the current Data Protection Directive:

- **Data minimisation:** this principle, which aims at limiting the amount of data collected for a specific purpose, is reinforced by requiring the collection to be limited to what is "**necessary**" in relation to the purposes for which the data is processed.
- **Accountability:** controllers and processors must be able to demonstrate compliance to Data Protection Authorities by **keeping a record** of certain types of processing activities. Consent is also subject to mandatory documentation provisions.
- **Transparency:** this principle is strengthened by setting **mandatory information** to be displayed and its format (clear and intelligible).

> "Under our Data Protection Policy, we have clearly expressed and defined explicit data retention guidelines and directives. These have been designed so that only the data we require to fulfil our business requirements is retained, and only for the duration that it is used to fulfil the specific purpose for which it was acquired".
>
> ***
>
> To address the specific requirements of the GDPR, Improve Digital has developed a new Data Protection Policy: data categories have been defined and implemented, clearly segregating the organisation's data according to type and protection requirements".
>
> **--- Improve Digital**

> "The first practical step was to order an audit from an external firm to have a broader and general look at all our activities on personal data. In parallel, we identified where we had personal data saved and registered across Europe, then we started mapping data flows.
>
> ***
>
> We revisited all our Terms and Conditions in December 2016 in order to make their content easy to understand for an average user. We produced a video with a famous presenter at RTBF to explain to users what we will be doing with their data, how they can control the data and what their rights are.
>
> ***
>
> We have other plans for early 2018, such as implementing the possibility for users to switch off content recommendations. We want users to be able to see the effects of algorithms, which is not possible on other platforms or social media. If you want to be transparent, you must help users to understand that there is something curating content for them. What we are also considering is to have an icon, a sign saying that the website (page) is curated by a machine, a computer".
>
> **--- RTBF**

IN PRACTICE:

Sales houses will need to ensure that their data processing activities comply with these principles by:

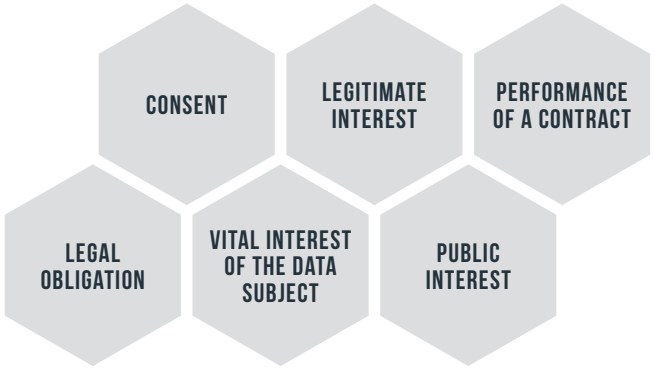
- Auditing their data processing activities, classifying processing partners and making sure that data processed is always linked to a specific purpose and is necessary for that purpose. For example, asking users for their year of birth instead of their full birthdate may be sufficient for targeting purposes while complying with data minimisation requirements;
- Updating their policies where necessary to inform users transparently on how their personal information is processed, in a clear and intelligible manner;
- Raising awareness and organising trainings internally to ensure that GDPR requirements are understood at every level and that day-to-day practices are adjusted accordingly;
- Documenting their data processing activities, in particular the collection of users' consent, to be able to demonstrate compliance to the Data Protection Authorities.

INITIATIVES BY EGTA MEMBERS:

- RTBF Video "charte de l'utilisateur RTBF": https://www.rtbf.be/charte/
- Channel 4's Viewer Promise video: http://www.channel4.com/4viewers/viewer-promise/our-viewer-promise

PART 03: GROUNDS FOR PROCESSING PERSONAL DATA

The list of legal grounds allowing the processing of personal data does not change:



However significant changes apply to the main legal basis used for **targeted advertising**:

Consent: to be valid, consent must be unambiguous, informed, specific and freely given.

- Unambiguous: **a clear and affirmative action** is now required to obtain a valid consent from the user. Silence, pre-ticked boxes or inactivity are no longer sufficient.
- Informed: the consent request and the nature of the processing must be presented in a manner which is **clearly distinguishable from other matters**, in an **intelligible** and easily accessible form, using **clear and plain language**.
- Specific: the data subject should be aware at least of the **identity** of the controller and the **purposes** for which the personal data will be processed, as well as the r**ecipients or categories of recipients** of the personal data[6].
- Freely given: consent is presumed not to be freely given:
  - where there is a **clear imbalance** between the data subject and the controller;
  - if the data subject has **no genuine choice** or is unable to refuse or withdraw consent without detriment;
  - and/or if the provision of a service is **dependent on** (consenting to) the processing of personal data despite such processing **not being necessary** for the provision of the requested service.

The last two bullet points cast a doubt on the future interpretation of a valid and freely given consent with regard to so-called "tracking walls", i.e. the capacity for website providers to block access to their content if users oppose the processing of their data for tracking purposes[7].

This will only be resolved through GDPR implementation. Should Member States or the Courts decide to adopt a restrictive interpretation of this provision, broadcasters and sales houses may have to adapt their business models (e.g. offering a pay-for alternative which may help qualify the consent as freely given).

- Withdrawal: users have the **right to withdraw consent** at any time and should be informed of this right.
- Children: processing childrens' data[8] requires **consent from the holder of parental responsibility**, although the GDPR does not specify how this consent must be obtained to be considered valid. Communication addressed at children must be easily understandable to them.
- Record: the controller shall be able to **demonstrate** that the data subject has consented to the processing of his or her personal data, i.e. consent must be documented.

> "The only legal basis which we use for advertising is consent".
>
> --- TF1

> "At Improve Digital we are adopting a marked emphasis on consent, as this best fits with our business and gives the data subjects transparency and control over their personal data".
>
> --- Improve Digital

Legitimate interest:

- Definition: the definition of legitimate interest is not substantially changed under the GDPR. It is clarified that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

> "Caution should be taken when claiming 'legitimate interest', as an incorrect assessment can result in an unlawful processing of personal data".
>
> --- Improve Digital

- Limitations: this legal basis should be considered with caution, as:
  - its use is conditioned to situations where "the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the **reasonable expectations** of data subjects based on their relationship with the controller";
  - the Article 29 Working Party has already deemed in the past that consent "**should be required**, for example, for tracking and profiling for purposes of direct marketing [and] behavioural advertisement"[9]. Such an opinion, although non-binding, can be used by the Courts to interpret the law, and the working party's role will be formalised under the GDPR as the European Data Protection Board;
  - the evolution of the **right to object** (see on the next page) has the potential to significantly obstruct the use of this legal basis;
  - the shift **from a Directive to a Regulation** will not give Member States as much room for interpretation as the text will directly apply across the whole EU instead of being transposed into national law.

> We still see legitimate interest as sufficient for some data use cases but we are additionally looking into the implementation of consent through a centralised log-in platform, especially as it is still unclear where the review of the ePrivacy Directive will lead us".
>
> --- RTL Mediengruppe

- Information: where "legitimate interests" are relied on in relation to specific processing operations, this will now need to be set out in **relevant information notices**.
- Record: controllers relying on "legitimate interests" should maintain a **record of the assessment** they made so that they can demonstrate that they gave proper consideration to the rights and freedoms of data subjects.
- Right to object: controllers should be aware that data processed on the basis of legitimate interests is subject to a right to object from the user - which **can only be rejected where there are "compelling" reasons** which override the interests, rights and freedoms of the data subject.

Performance of a contract: this legal basis has not changed. It allows the processing of personal data:

- Where processing is **necessary** for the performance of a contract to which the data subject is a party – e.g. processing location information or credit card details necessary for making the payment and delivering goods ordered online;
- Where the processing of personal data takes place prior to entering into a contract. In that case, the processing of data generally serves the purpose of **answering a direct request** from the user. For example, if a user asks for a quote for his/her car insurance, the processing of that person's personal data could be permitted to answer this particular question.

> In 2015, we launched a public tender to implement a Single Sign-On (SSO) system for our websites and applications, which is the basis of our architecture to comply with the GDPR. This means that our users have to register (free registration) if they want to use certain services (e.g. to watch a live show or a football game). This system was launched in December 2016. It allows us to identify and capture all the data in one place, but also to better understand our users' needs to provide them with better content and therefore better fulfil our public service mission.
>
> ***
>
> We have defined different age classes. Below 13, we don't do content recommendation or targeted advertising (although they can still see non-targeted advertising). Over 16, you may be exposed to targeted advertising. This is all indicated in our terms and conditions. In order to check the age, we are discussing a potential safeguard such as requesting the birthdate on a declarative basis"[10].
>
> --- RTBF

> We are in the process of founding a consent platform (log-in alliance), starting with ProSiebenSat.1 and United Internet plus Zalando as the first partners to implement a single sign-on-platform and obtain permissions/consent".
>
> --- RTL Mediengruppe

IN PRACTICE:

The GDPR is yet to be implemented and many of its provisions are still subject to interpretation by Data Protection Authorities and the Courts. However, it does seem that the **legal bases regularly used for interest-based advertising are being restricted to some extent in the GDPR**, in comparison with the current Data Protection Directive.

Consent is still the main legal basis used by broadcasters, and the reinforcement of the provisions on consent, as well as new requirements introduced in the GDPR (such as, among others, the right to data portability) have prompted some broadcasting companies to develop **single sign-on solutions** (centralised log-in system across several services).

Regarding children's consent, sales houses will need to put in place **mechanisms to check users' age** and ask for parental consent when necessary.

It should also be noted that online advertising may, under certain circumstances, fall under **article 22** on automated decision making and profiling, which further restricts the use of certain legal bases (mainly legitimate interest). [see Article 29 WP Guidelines on profiling].

PART 04:

CONTROLLERS AND PROCESSORS

- Definition: the definitions of controller and processor remain **unchanged**. Entities that are controllers or processors should continue to be considered so under the new Regulation.

  The **controller** is the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

  The **processor** is the natural or legal person which processes personal data on behalf of the controller.

> "Improve Digital considers itself a controller and a processor, depending on each specific data flow and the relevant (legal) factors concerned. But it should be kept in mind that labelling yourself as a processor is in itself not decisive: practice (what happens in reality) determines which position (controller/processor) you take".
>
> --- Improve Digital

> "The companies within TF1 Group are positioned as data controllers. We plan a contractual audit to update the agreements in order to clarify our partners' responsibilities".
>
> --- TF1

- Identification: the notion of controller or processor is dependent on each company's situation and the nature of the data flows.
- Processors' obligations: the GDPR imposes **new requirements** for all data processing agreements between controllers and processors.
  - Processors must keep a **record** of data processing activities carried out on behalf of the controller;
  - They must implement measures to **help the controller** fulfil its obligations regarding data subjects' rights;
  - Processors must assist controllers in their **cooperation with data protection authorities**.
- Liability: unlike in the current Directive were processors were mostly exempted from liability, **the GDPR will apply directly to processors**. This is a significant change, although some Member States had already placed some direct obligations on processors in their national laws.
- Joint controllers: the GDPR imposes obligations on joint controllers, which are defined as two or more controllers who jointly determine the purposes and means of processing. The joint controllers should determine their respective responsibilities for compliance under an "**arrangement**" between themselves and inform individuals accordingly.

> "We have analysed our role and obligations for each of the external entities we deal with. Whereas ascertained by the data flow we fall within the Data Processor role, we have looked to map our internal Privacy Management Activities to the language of the contract that governs that relationship. Where we fall under the role of Data Controller, we look to enforce our Privacy Management Activities through the contracts we hold with other entities. In the case where we carry joint roles then the rationale employed is a combination of the two previous roles".
>
> --- Improve Digital

IN PRACTICE:

These new requirements will complexify contract negotiations with processors. Controllers should consider whether they need to **update their contracts** with existing suppliers to abide with the new requirements.

In particular, it could be useful to define within the contract what is the **scope of the processor's responsibilities** and potential liabilities in case of compensation claims, given that processors are now directly liable under GDPR.

Instances of joint controllers may be frequent in group companies, for example between a channel and a sales house, so egta members need to be aware of their responsibilities in that situation.

PART 05: ENHANCED RIGHTS OF DATA SUBJECTS

The main changes compared to the current Data Protection Directive are listed below:

- Right of access to one's personal data: this right is **strengthened**. Users can obtain information about the period for which the personal data will be stored, or about the source of the data when it was not collected from them. In certain cases, users also benefit from a right to restrict processing of this data.
- Right to erasure ('right to be forgotten'): essentially, data subjects can ask for erasure of their personal data if it is **no longer needed for its original purpose** or if **lawful grounds for the processing no longer exist** (e.g. withdrawal of consent or objection to the controller's legitimate interest) and no alternative purpose or legal basis can justify the processing. If the personal data has been made public, the controller must **take all reasonable steps** to inform other controllers processing the personal data that the data subject has requested its erasure.
- Data portability: through this new right, data subjects can demand that the personal data they provided to a controller be **transmitted to them or a new provider** in machine-readable format. This right is actionable where the processing is based on consent or the performance of a contract, and if the processing is carried out by automated means.
- Right to object to the processing of personal data:
  - based on **legitimate interest**;
  - and/or **for direct marketing purposes**.

  The **burden of proof is reversed**, as the controller must now cease processing the personal data unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject.

  The text also makes clear that this right should be **explicitly brought to the attention of the data subject** and presented clearly and separately from any other information.
- Deadline: demands regarding users' rights must be met within **one month** from the reception of the request and the original answer must be provided free of charge.
- Burden of proof: controllers refusing to act on a request related to users' rights shall bear the burden of **demonstrating the manifestly unfounded or excessive character of the request**.

> "We plan to update our data protection policy to include the new rights of the people concerned. However, mapping out all the necessary actions for compliance will of course lead to new expenses, currently assessed internally".
>
> --- TF1

> "One fundamental element of our consent platform will be a privacy centre that will meet the requirements of transparency as well as data portability".
>
> --- RTL Mediengruppe

> "Data erasure is already in place through the single sign-on system, it's a one-click operation. Regarding data portability, we discussed the possible formats with the European Commission during summer 2017 and they want to leave it up to the industry to agree on a common standard, however there is none today".
>
> --- RTBF

IN PRACTICE:

Compliance to users' rights will become more onerous due to:

- the limited timeframe for answering users' request;
- the obligation to provide an answer free of charge;
- the necessary investments to ensure the activation of the new right to data portability as well as the extension of the right to be forgotten which will likely cause a multiplication of requests.

The evolution of the right to object risks disturbing the use of legitimate interest in the field of targeted advertising as well as direct marketing. It is likely that the number of objections will increase, and it will be more burdensome for companies to justify each individual processing activity.

Similarly to the consent requirements, a single sign-on model can be a useful tool to implement the new users' rights.

PART 06:

DATA GOVERNANCE RULES

The GDPR integrates a number of organisational/ structural requirements.

- Data protection by design and by default: controllers must be able to show that they have implemented **state-of-the-art technical and organisational measures** (pseudonymisation being one) to implement data protection principles and protect the rights of data subject. These measures can **vary according to the risks** of the processing activities on the rights and freedoms of natural persons, as well as the cost of implementation.
- Data Protection Impact Assessments (DPIAs)[11]: DPIAs are required when a type of processing is likely to result in a **high risk** to the rights and freedoms of natural persons.

  The GDPR does not clearly classify targeted advertising techniques used by broadcasters as activities requiring DPIAs, however it is likely that they will be necessary. The Article 29 Working Party has proposed a list of nine criteria[12] to be taken into account when assessing this, including some which are **directly relevant to targeted advertising**:

  - the controller evaluates and scores, including profiling and predicting, "*especially from aspects concerning (...) personal preferences or interests, reliability or behaviour, location or movements*";
  - the controller processes data on a large scale;
  - data sets have been matched or combined;
  - the data concerns vulnerable data subjects (including children);

> "What seems to be the biggest challenge is the practical implementation of new concepts that are somewhat abstract for operators – such as security by default, privacy by design, accountability – in a context where we are waiting for guidelines from regulatory bodies, and for the adoption of the e-Privacy Regulation that will inevitably have an effect, in particular on the way we receive a user's consent before the installation of the tracker on his/her terminal."
>
> **--- TF1**

> "The single sign-on system is not only meant to comply with consent, it is also a useful tool in moving towards privacy by design. With this system, the user can literally stop data being collected with one click".
>
> **--- RTBF**

  - innovative technological or organisational solutions are used.

The minimal content of a DPIA is specified as follows:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes, as well as of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

Please note that additional requirements may apply, such as mandatory consultation of the supervisory authority in specific cases.

- Data Protection Officers (DPOs): the designation of a DPO is mandatory, among other situations, when the core activities of the controller or the processor consist of processing operations which require **regular and systematic monitoring of data subjects on a large scale**. This should cover the processing of personal data for behavioural advertising purposes.

  DPOs' tasks will include:

  - **Advising** their colleagues of their obligations under GDPR, including via training and awareness raising, as well as regarding DPIAs;
  - **Monitoring** their organisation's GDPR/ privacy law compliance (e.g. by running audits);
  - **Cooperating** with and acting as the contact point for supervisory authorities.

  Controllers and processors must:

  - Ensure that their DPO is **involved in all issues related to the protection of personal data**;
  - Provide **adequate resources** necessary to carry out the DPO's tasks;
  - Ensure that their DPO **reports directly to the highest level of management**.

  The DPO can either be a member of staff or a hired contractor; group companies can appoint a single DPO.

  The Article 29 Working Party's guidance stresses that DPOs will not be personally liable for their organisation's failure to comply with the GDPR[13]: data protection is the responsibility of the controller or the processor.

  The GDPR does not restrict DPOs from holding other posts but expressly requires that such other tasks must **not create a situation of conflict of interest** for the DPO. According to the Article 29 Working Party, conflicting positions within the organisation may include senior management positions (e.g. CEO, COO, CFO, CMO, Head of IT Department) and other positions which may lead the DPO to 'determine the purposes and the means of the processing of personal data'.

> "We appointed a DPO who reports directly to the Executive Management team and is the authority for Information Security and Data Protection within our company".
>
> **--- Improve Digital**

> "On the basis of the methodology developed with the assistance of internal experts, TF1 already took some actions, including the organisation of information sessions aiming at raising the awareness of all colleagues on personal data protection. We also updated internal rules such as our general policy for personal data protection, set up processes to handle new users' rights and prepared our teams for the new obligations regarding Data Protection Impact Assessments".
>
> --- TF1

IN PRACTICE:

Given the **high level of potential sanctions** sales houses should remain cautious by undertaking any necessary steps to demonstrate compliance.

As an example, failure to carry out a DPIA when required, or carrying out a DPIA in an incorrect way can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Also, some changes foreseen (e.g. privacy by default) may imply more radical **organisational changes**. From May 2018, the protection of personal data will likely affect every media/advertising professional's day-to-day work. **Trainings and awareness-raising** are part of the necessary steps to go through in order to ensure an appropriate adjustment of business structures to ensure compliance with the new data protection rules.

PART 07:

COMPLIANCE TOOLS: CODES OF CONDUCT AND CERTIFICATION MARKS

- Codes of Conduct are reinforced.
  - They can be **drafted by associations or other industry bodies** and can relate to general or specific aspects of the GDPR;
  - Controllers and processors outside the European Economic Area can adhere to an approved Code of Conduct to provide the basis for Cross-Border Data Transfers;
  - Data Protection Authorities (DPA) can appoint an **independent body** to monitor and enforce a Code of Conduct. Although the DPA remains the lawful enforcer, this may allow industry bodies to collaborate and bring sector-specific expertise;
  - Codes of conduct will be considered as a **positive factor in a DPIA** and **may affect any fines** imposed upon the adherent controller or processor;
  - They can cover a wide range of topics such as legitimate interest or pseudonymisation. They must be **approved and published by the competent DPA**, which can decide to amend it if does not provide sufficient protections.
- Certification Mechanisms (seals/marks) are introduced at European level
  - Their objective is to provide a formally recognised **proof of compliance with the GDPR**, typically with an associated visual sign (e.g., an icon or emblem to be displayed);
  - Although **voluntary**, they will allow controllers/processors to demonstrate compliance with the GDPR requirements, e.g. in terms of data protection by design and by default;
  - They will remain valid for **three years**, then will need to be renewed;
  - They are **enforced by the DPA or by an independent body accredited by the DPA** that oversees the relevant scheme.

IN PRACTICE:

Members of trade associations or similar sector specific bodies should monitor the creation of codes of conduct, which might impose particular additional requirements.

In the future, certification seals or marks may be used as means of **differentiation with competition**, as they will give users **additional guarantees** that their personal data is adequately protected.

PART 08:

TRANSFERS TO THIRD COUNTRIES

The current requirements remain **largely unchanged**. The GDPR allows for the transfer of personal data to third countries or international organisations under the following conditions:

- 'Adequacy decision' from the European Commission:
  - Decision with legal effect establishing that a non-EU country provides a level of data protection that is "**essentially equivalent**" to that in the EU;
  - The effect is to enable the free flow of personal data to that third country without the need for the data exporter to provide further safeguards or obtain any authorisation. Transfers to the country in question will be assimilated to intra-EU transmissions of data.
- In the absence of an adequacy decision:
  - Standard Contract Clauses (SCC): adopted or approved by the European Commission, they lay down the **respective data protection obligations** between the EU exporter and the third country importer;
  - Binding Corporate Rules (BCR): **internal rules** adopted by a multinational group of companies to carry out data transfers within the same corporate group to entities located in countries which do not provide an adequate level of protection (already in use under 1995 Directive, but their role is formalised). BCR can now be used by a group of enterprises engaged in a joint economic activity but not necessarily forming part of the same corporate group;

    The new law **abolishes general requirements of prior notification** to and authorisation by DPAs of transfers to a third country based on these two tools (SCCs and BCRs);
  - Approved Codes of conduct and Certification mechanisms will also be an option for compliance, provided that they include **binding and enforceable commitments** by the controller or processor in the third country to apply the appropriate safeguards;
- In the absence of any of the above, derogations allow the transfer of personal data to a third country in certain conditions: for example, **when the data subject has explicitly consented to the proposed transfer** or when the transfer is necessary for the performance of a contract between the data subject and the controller.

IN PRACTICE:

Existing Binding Corporate Rules or Standard Contract Clauses remain valid until amended, replaced or repealed in accordance with the GDPR.

Regarding data transfers to the United States, the EU does not list the U.S. as one of the countries that meets its data protection requirements. However, a bilateral agreement ('Privacy Shield') implemented from 1st August 2016 created a legal mechanism whereby U.S.-based companies can benefit from an adequacy recognition. To join the Privacy Shield Framework, a U.S.-based company must voluntarily self-certify to the Department of Commerce and publicly commit to comply with the Privacy Shield Principles. Once made public, the commitment becomes enforceable under U.S. law.

PART 09:

DATA BREACH NOTIFICATION

- The GDPR introduces a personal data breach notification regime, which applies in case of "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".
- Controllers must notify personal data breaches to Data Protection Authorities **without undue delay** and, where feasible, **within 72 hours** after becoming aware of it. They must document any personal data breach.
- Processors must notify personal data breaches to controllers without undue delay.
- When the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Certain exemptions apply where:
  - sufficient technical and organisational measures were in place to protect the personal data, such as encryption rendering the data unintelligible to any unauthorised party;
  - the controller can take subsequent measures to avoid the high risk to materialise;
  - or if the communication would involve a disproportionate effort (it can then be replaced by a public communication).

IN PRACTICE:

Sales houses should ensure that appropriate procedures are in place in order to:

- **minimise the impact** of any data breach, for example by using encryption tools;
- **communicate smoothly** any data breaches to the relevant data protection authority within the appropriate timeframe, in particular by informing their IT departments of the legal obligations under GDPR;
- ensure that **agreements with processors** include information duties to enable the controller to comply with its obligations regarding data breach reporting. In many cases, the controller will depend on its processors' proactivity.

PART 10:
SANCTIONS

The GDPR radically increases the level of economic sanctions against infringing controllers and processors of personal data.

- Individuals have a **right to compensation** from controllers or processors for any material or non-material damage resulting from an infringement of the GDPR;
- Data protection authorities are empowered to impose administrative fines which can reach **€20 million or 4% of global turnover**, whichever is higher;
- Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the **right to an effective judicial remedy** against a legally binding decision of a supervisory authority concerning them.

IN PRACTICE:

The level of potential sanctions should encourage companies to adopt a cautious approach and to carry **in-depth and regular assessments of their compliance with the GDPR**.

This is reinforced by the fact that sanctions may be mitigated, taking into account several factors including actions showing negligence of the infringing organisation or, conversely, the existence of appropriate technical and organisational measures[14].

REFERENCES:

1. *For example, one study showed that 87% of Americans can be individually identified by combining three indirect identifiers: date of birth, gender and ZIP code; available at: http://dataprivacylab.org/projects/identifiability/paper1.pdf.*
2. *As ruled in the Breyer case by the Court of Justice of the European Union (C-582/14); available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5a2d8c2ba77f14eb29957f420c8230c79.e34KaxiLc3eQc40LaxqMbN4PaNOTeO?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1368662.*
3. *Such as privacy by default (article 25(1)), security of processing (article 32(1)) or to justify further processing of personal data (article 6(4)e).*
4. *Hashing is using a mathematical function to pseudonymise a piece of content/information.*
5. *Internet Advertising Bureau Europe - Working paper on the definition of personal data; available at: https://www.iabeurope.eu/wp-content/uploads/2017/07/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf.*
6. *It should be noted that some Data Protection Authorities are questioning whether even well-described categories of controllers may not suffice for obtaining informed consent. In the Netherlands (under the current Dutch Privacy Laws) the DPA is of the opinion that all recipients of the personal data must be named specifically; categories are not sufficient. The guidance of the United Kingdom's Information Commissioner Office on consent also seems to follow the same interpretation. This is in contrast to the information disclosure prescriptions of Arts. 13-14 GDPR, which only state that "recipients or categories recipients of the personal data" must be disclosed.*
7. *As an example, the UK Information Commissioner's Office's draft guidance on consent, although non-binding, seems to interpret these provisions in a restrictive way, which could render tracking walls unlawful in the near future.*
8. *The GDPR defines a child as under 16 years old, but Member States can individually decide to lower the limit to 13 years old. A good overview of what limit has been set by individual Member States is available here: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355*
9. *Article 29 Working Party - Opinion 03/2013 on purpose limitation, p.46.*
10. *Available at: https://www.rtbf.be/charte/detail#enfantplus.*
11. *Note: the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.*
12. *See the Article 29 Working Party's Guidelines on Data Protection Impact Assessment, p.9; available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.*
13. *See Guidelines on Data Protection Officers ('DPOs'), p.24; available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.*
14. *For more detailed information, see the Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679; available at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.*

ANNEX – USEFUL SOURCES

General overviews on the GDPR:

- DLA Piper – A guide to the General Data Protection Regulation; available at: https://www.dlapiper.com/~/media/Files/Insights/Publications/2016/12/General Data Protection Regulation Brochure.PDF.
- Baker & McKenzie – EU General Data Protection Regulation in 13 game changers; available at: http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-GDPR%20Game%20Changers%20Booklet.pdf.
- Bird & Bird – Guide to the General Data Protection Regulation; available at: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en.
- Allen & Overy – The EU General Data Protection Regulation; available at: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.
- White & Case – Unlocking the EU General Data Protection Regulation; available at: https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation
- Internet Advertising Bureau Europe – GDPR compliance primer; available at: https://www.iabeurope.eu/wp-content/uploads/2017/06/20172205-IABEU-GIG-Working-Paper01_GDPR-Compliance-Primer.pdf.
- World Federation of Advertisers – GDPR Guide for marketers; available at: https://www.wfanet.org/news-centre/gdpr/.

Personal data:

- Article 29 Working Party:
  - Opinion 4/2007 on the concept of personal data (interpretation of the current Data Protection Directive); available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
  - Opinion 5/2014 on anonymisation techniques (interpretation of the current Data Protection Directive); available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
- Internet Advertising Bureau Europe – Working paper on the definition of personal data; available at: https://www.iabeurope.eu/wp-content/uploads/2017/07/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf.
- International Association of Privacy Professionals – Top 10 operational impacts of the GDPR: Part 8 Pseudonymisation; available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

Consent:

- Future Article 29 Working Party Guidance on Consent (still to be released).
- Information Commissioner's Office – Draft Guidance on consent (final version planned for December 2017); available at: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

Legitimate interest:

- Article 29 Working Party – Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC (interpretation of the current Data Protection Directive); available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
- Data Protection Network – Guidance on the use of legitimate interest under the EU General Data Protection Regulation; available at: https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf.
- Slaughter & May – Processing of personal data: consent & legitimate interests under the GDPR; available at: https://www.slaughterandmay.com/media/2535723/processing-of-personal-data-consent-and-legitimate-interests-under-the-gdpr.pdf.

Controller and processor:

- Article 29 Working Party – Opinion 1/2010 on the concepts of "controller" and "processor"; available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Users' rights:

- Article 29 Working Party – Guidelines on the right to "data portability"; available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
- Future guidelines from the Article 29 Working Party on transparency (still to be published).

Profiling:

- Article 29 Working Party – Provisional Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (still subject to modifications following a public consultation ending on 28th November 2017); available at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.

Data governance rules:

- DPIA:
  - Article 29 Working Party – Guidelines on Data Protection Impact Assessment; available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.
- DPO:
  - Article 29 Working Party – Guidelines on Data Protection Officers ('DPOs'); available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

Data breach notification:

- Article 29 Working Party – Provisional Guidelines on personal data breach notification (still subject to modifications following a public consultation ending on 28th November 2017); available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741.

Sanctions:

- Article 29 Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679; available at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

MORE ON THIS TOPIC

Editorial Committee:

Conor Murray
Regulatory & Public affairs Director
E: conor.murray@egta.com
T: + 32 2 290 31 36

François Lavoir
European Affairs Policy Advisor
E: francois.lavoir@egta.com
T: + 32 2 237 60 40

Alain Beerens
Marketing and Communication Manager
E: alain.beerens@egta.com
T: + 32 2 290 31 38

Design:

Paulina Kott
Head of IT & Design
E: paulina.kott@egta.com
T: + 32 2 290 31 33

MORE ON EGTA

egta - association of television and radio sales houses

egta is the Brussels-based trade association of more than 140 television and radio advertising sales houses. egta's members are spread across 40 countries, mainly in Europe. Together, egta's TV members represent over 80% of the European television advertising market, whilst egta radio members collect 60% of radio advertising revenues in countries where they are active.

As sales houses of both public and private broadcasters, egta members commercialise the advertising space around audiovisual content available on platforms such as traditional television and radio sets, tablets, smartphones, PCs, Smart TVs and other Internet-connected devices.

egta.

22, Rue des Comédiens, boîte 4
1000 Brussels - Belgium
T: + 32 2 290 31 31
www.egta.com
@egtaconnect

egta.

www.egta.com