EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

What AGENCIES should know about THE GDPR

LIST OF CONTENTS

ABOUT US

The European Association of Communications Agencies (EACA) represents more than 2,500 communications agencies and agency associations from 30 European countries that employ more than 120,000 people. EACA members include advertising, media, digital, branding and PR agencies.

EACA promotes honest, effective advertising, high professional standards and awareness of the contribution of advertising in a free market economy. We encourage close co-operation between agencies, advertisers and media in European advertising bodies. EACA works closely with the EU institutions to ensure freedom to advertise responsibly and creatively.

We are here to share and address international experience and issues on a pan-European basis and provide an important link between agencies, advertisers and the advertising media in Europe and around the world.

Co-author:

Aurélie Pols (Data Governance & Privacy Engineer, DPO Trainer for the GDPR) designs data privacy best practices: documenting data flows, minimising risk related to data uses, solving for data quality.

She spent 18 years optimising digital data-based decision-making processes. She co-founded and sold her start-up to Digitas LBi (Publicis). Used to following the money to optimise data trails, she documents data flows to minimise risks, touching upon security practices and ethical data uses. She leads her own consultancy, is part of the EDPS' EAG and served as Data Governance & Privacy Advocate for Krux Digital (Salesforce).

Aurélie has been teaching Privacy & Ethics at IE Business School in Madrid for 5 years and supports DPO training courses for Maastricht University and co-chairs IEEE's P7002 (Data Privacy Process).

@AureliePols

eaca
EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

ABOUT THIS PAPER

In the final months and weeks leading up to the adoption of the General Data Protection Regulation (GDPR), it is important for agencies to be on top of the game. Not for a long time has such a significant piece of European regulation penetrated the business practices of advertising agencies. The GDPR will affect targeted marketing campaigns, imposing new rules on how personal data is to be handled and what internal procedures must be in place to ensure at least compliance and certainly risk minimisation.

Are you confident that you will satisfy the conditions of the new Regulation **from 25 May 2018** onwards? And are you aware of the next piece of European data protection legislation (ePrivacy) currently being negotiated by the EU institutions?

EACA has collected a set of pointers for its members to read through in order to make sure that the key changes brought by the upcoming legislation are addressed in time. Furthermore, some lines are included on the likely content of the ePrivacy Regulation, as known at the time of publishing of this report. The ePrivacy Regulation is an accompanying and specified set of rules to the GDPR - also called lex specialis: the GDPR applies unless specified otherwise in ePrivacy - applicable specifically in electronic communications.

The guidelines 'What agencies should know about the GDPR' are partly based on a webinar of the same title organised by EACA on 13 December 2017. A recording is available here. The presenter is Aurélie Pols, Data Governance and Privacy Engineer and Data Protection Officer Trainer for the GDPR. She is also the co-author of this publication. The webinar and this report aim to highlight the main changes agencies need to be aware of and prepare themselves for the GDPR.

These guidelines are not intended to constitute legal advice but rather to complement it. EACA disclaims any liability in connection with the use of the information provided in this document. The information contained in this document has been written in February 2018 and may be subject to change. We highly recommend that you create GDPR-proof data processing strategies with the help of your legal, risk, compliance and data teams. You may also consult your national data protection authority (which will become national supervisory authorities under the GDPR).

KEY FACTS AT A GLANCE

The General Data Protection Regulation (GDPR) will replace the existing legislation applicable to data processing carried out by communications agencies. It will impact the way agencies use data to build and deliver campaigns. Here's a quick summary of what agencies should know:

When?

Already applicable, enforceable as of 25 May 2018.

Who does it concern?

All entities that control and process personal data of 'data subjects who are in the Union' if they offer any goods or services, even free ones, or monitor their behaviour, regardless of geographical location.

Penalties?

Infringers can be liable for up to 4% of their global turnover or 20 million € - whichever is higher.

Who is who?

The entity defining the purpose and means of data processing is the data controller, typically agencies' clients. A data processor acts on behalf of the data controller, through written instructions and their relationship is governed by a contract. If a processor determines another purpose for the use of data – even if pseudonymised, hashed &/or encrypted - it becomes a controller. In the GDPR, there is a new notion of joint controllers, where two or more controllers determine the purposes and means of processing to rebalance possible power asymmetries.

On what basis can data be processed?

There are 6 legal grounds to assure lawfulness of processing under the GDPR as defined in Article 6. Typically the data controller defines the purposes for which processing takes place as well as the legal ground used. Most probably those preferred by the sector will be either consent or legitimate interests, unless otherwise specified by the client. Note that legitimate interests are not an option available within the current ePrivacy Regulation draft.

How can consent be obtained?

When selected as a legal ground for processing, the conditions for consent are defined in Article 7 of the GDPR. Detailed records of consent must be kept allowing the data controller to demonstrate compliance, according to the 'accountability' principle. Consent should be separated from other data processing endeavors such as terms and conditions and it should be 'clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language'. Consent can be withdrawn at any time, and such withdrawal should be as easy as giving it in the first place and consent should be given freely.

Children?

Verifiable parental consent must be obtained for children aged below 16. Member states can define a lower threshold. The consensus is typically 13 to also allow for alignment with the US-based COPPA. Check your local transposition, some countries remain at 14 at the time of writing.

Information to data subjects (consumers)?

Data controllers have an obligation to provide detailed information about data processing to data subjects as soon as data is collected. It should be immediately apparent to the consumers where to find this information and it should at least include: who processes the data, how to complain about this, why such data is processed in the first place, who else gets the data and whether the data leaves the European Economic Area.

Data breach?

If a data breach results in a 'high risk', the data controller has an obligation to notify the supervisory authorities within 72 hours. A data processor has an obligation to notify the controller without undue delay. Depending on agencies' contracts with their clients and the gravity of the situation, they might need to assist.

Impact assessment?

You may have an obligation to conduct a data protection impact assessment if processing is likely to result in a 'high risk'. Guidelines by the Article 29 Working Party further specify high risk. Data protection impact assessments are an opportunity to document data processes and agree on remedial measures to assure a risk-based approach to data processing and prove compliance with the GDPR.

Consumers'/data subjects' rights?

Consumers' position is strengthened. Consumers will have new rights such as the right to erasure (to be forgotten), the right to restriction of processing, the right to data portability, and the right not to be subject to automated individual decision-making, including profiling. Other existing rights are reinforced such as the rights to be informed, of access, to rectification and to object.

Data Protection Officer?

You may need to appoint a data protection officer if your core activities consist of processing operations, which require regular and systematic monitoring of consumers on a large scale or involve special categories of data or related to criminal convictions and offences. Agencies working in the health sector, active for political operatives, involved in trade union membership or religious movements are advised to seek further counsel and document their decisions.

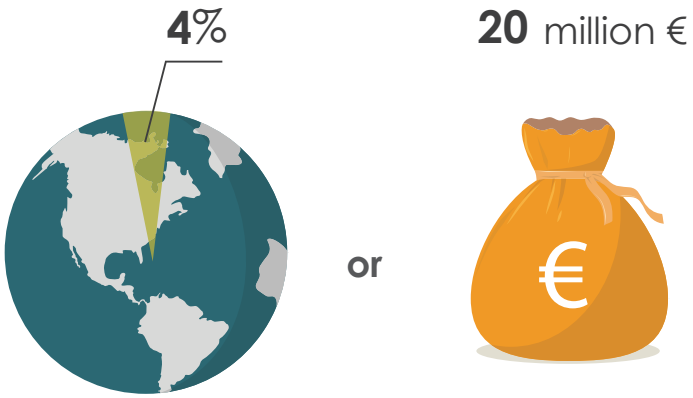
1

DOES THE GDPR APPLY TO ME?

At the European level, the main piece of legislation currently governing the processing and transferring of personal data is Directive 95/46/EC. After nearly 23 years, the European Union is bringing into force new rules in the form of the General Data Protection Regulation, which comes into force in all the member states from 25 May 2018 onwards, including the UK for now and the remaining countries of the European Economic Area: Norway, Lichtenstein and Iceland. Reflecting the public's increased need for more transparency and building upon the existing Directive, it defines the new baseline for compliance.

The end result is that more rights will be given to citizens and consumers - 'data subjects' - to control how companies can process their data. Companies – including agencies – also have more responsibilities.

In cases of data breach, your company may be liable for **4%** of its global turnover or **20 million €** - whichever is higher.



The scope of the legislation expands responsibilities from data controllers alone to companies that are data processors acting on behalf of controllers. As discussed in more detail in the next section, advertising agencies typically occupy the role of processors.

There is also a broader range of what is considered personal data under the GDPR. The recitals highlight that certain categories of online data may be personal data – online identifiers, device identifiers, cookie IDs and IP addresses are referenced. Such identifiers will be personal data where used to create profiles of people and identify them.

Furthermore, if you are an agency or an agency association outside the EU, you may need to comply with the rules and appoint a representative in the EU. The new GDPR rules catch data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour (within the EU) of 'data subjects who are in the Union'. The legislation shifts focus on where the data is processed to who the data is about, i.e. data subjects.

ACTION POINT
Find out whether your agency processes personal data of data subjects who are in the Union. If yes, the GDPR applies to you!

2

AM I A DATA CONTROLLER, A DATA PROCESSOR OR A JOINT CONTROLLER?

The exact liabilities of the GDPR will depend on which role your agency has under the new legislation. Every part of the supply chain that 'touches' data will need to understand their role. The following three main roles have been identified in the GDPR's data ecosystem:

Data subject - individuals whose data is processed

Data controller - 'alone or with others determines the purposes and means of processing personal data'[1]

The clients of advertising agencies typically occupy the role of data controllers. They define the purposes for which the data is processed in the first place and ask processors what is being collected, where and by whom, and to document all of the information. Under the GDPR, they have the most responsibilities.

Data processor - 'processes data on behalf of the Controller'[2]

Agencies are normally processors, helping behind the controller. However, there is a possibility of being a joint controller and processor. With this regard, it is important to look at the purpose of data processing and whether the agency is doing more with the data than what the controller specified. If an agency pseudonymises data and creates a general pool of information about how consumers use certain services that is used across different clients, it may become a joint-controller.

Media owners, on the other hand, are typically data controllers as they define the purpose for the processing operations and use tools to process their data. Such tools, through their multiple product and feature integrations, could repurpose the data under the cover of 'data anonymisation' practices such as hashing and/or encryption. Independent of the techniques used, they still repurpose the data and therefore become joint controllers.

ACTION POINT

Identify whether you are a data controller, a data processor or a joint-controller. Agencies typically want to be classified as data processors and avoid the burdens of being a controller. Find ways to prove it and maintain the status unless you make an active choice to revise the policies and notices.

ACTION POINT

Update the contracts between controllers and processors to clarify roles, responsibilities and allowable processes.

Controllers will need to consider the type of data held by themselves and Processors:

- Why is it being held?
- Where is it being held?
- Who is using it?
- How is it being used?

Paperwork to clarify the answers will be essential. Make sure that the contracts between you and your clients align with one another and that data is used in a secured way.

Once you know who you are, the responsibilities are discussed in Articles 25, 26 and 28 (see the Annex). [3]

3

WHAT ARE THE LAWFUL BASES FOR PROCESSING DATA?

The possible bases for processing data are:[4]

- Consent
- Performance of a contract
- Necessary for compliance
- In order to protect vital interests
- Necessary for the performance of a task carried out in the public interest
- Legitimate interests

For advertising, typically **consent** or **legitimate interests** are used.

The requirements for consent are discussed in more detail in section 5. Legitimate interests could exist and would require at least the data subject to be directly linked to the data controller. This would allow for alignment of the reasonable expectations of the data subject to the processing of the personal data. The processing of personal data for direct marketing purposes may be regarded as carried out on the basis of legitimate interests, but would require a balancing test.

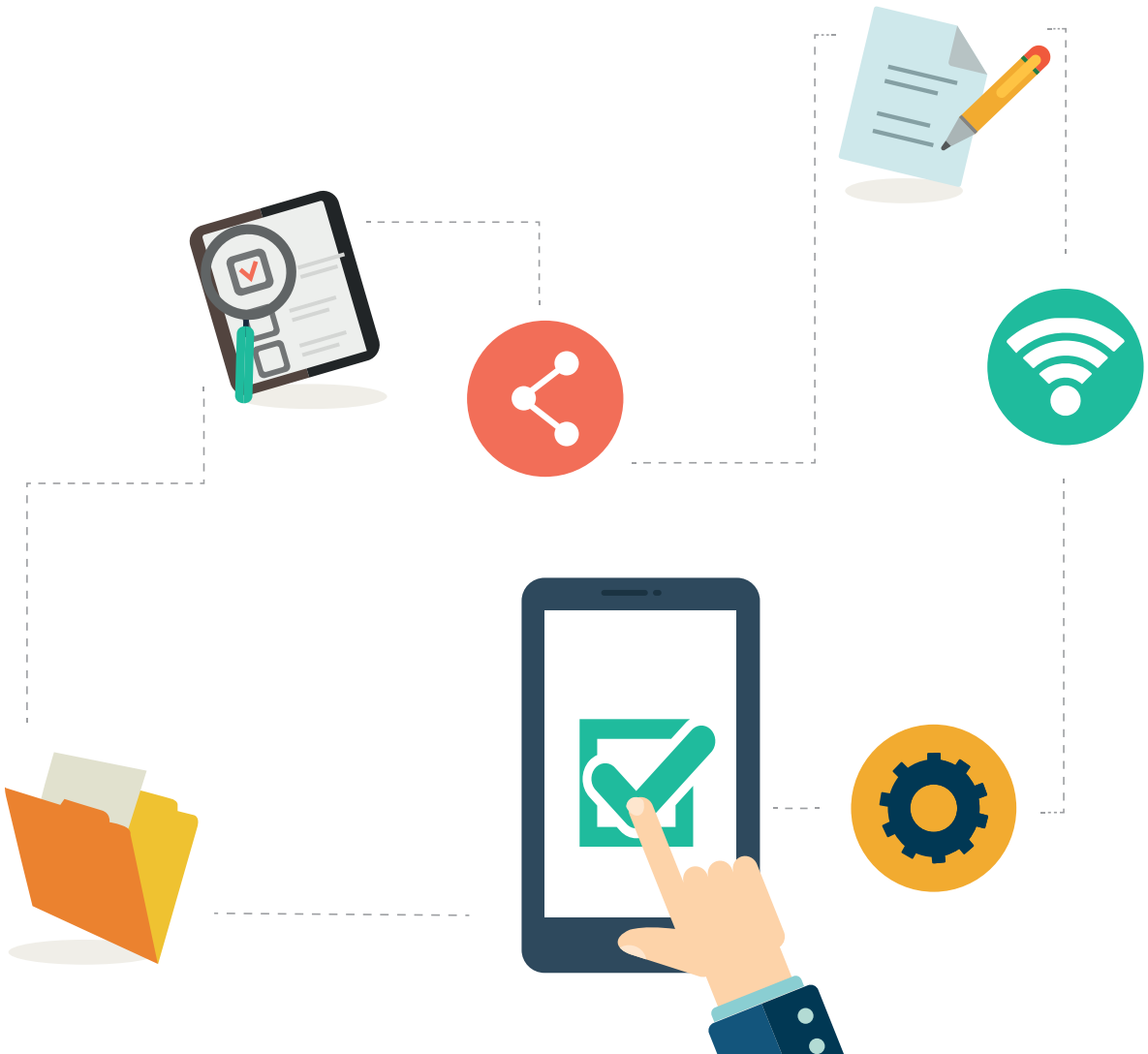
It is worth noting that if data is anonymous, no privacy legislation applies. It is an ideal card to get out of the privacy legislation but not very robust to rely on, as proving total and continuous anonymity of data remains a challenge. Anonymising data is different from pseudonymising data. Pseudonymised data means 'that the personal data can no longer be attributed to a specific data subject without the use of additional information', typically applying technical and organisational measures to separate the original data from the pseudonymised data. The key to re-identify individuals is kept separately. This data still falls within the scope of the GDPR but can help companies to rely on the legitimate interests legal ground by demonstrating balancing tests. Pseudonymisation is seen as a good mitigation practice to limit risks related to data usage while not being a wildcard to get out of any obligations with respect to the GDPR. Obligations such as breach notifications of data subjects' rights might still apply.

The problem with pseudonymous and also anonymous data is that as more data are added, outliers tend to appear which could, theoretically, re-identify data subjects. This was the case with a dataset Netflix released of 500,000 customers where researches identified users by cross-referencing data.

While the GDPR doesn't define anonymous data, the current Directive does and states 'whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or any person to identify said data'.[5] This hints at an increase in risk of re-identification in case the data is kept or enriched. Ideally, anonymous data should be used for its purpose and after the use be disposed of to mitigate risk.

Note that the Future of Privacy Forum's Visual Guide to Practical de-identification might also be a starting point to develop best practices around de-identification and anonymisation techniques.[6]

ACTION POINT
Analyse which legal base you will use to process data under the GDPR.



4

GDPR vs. ePRIVACY

The ePrivacy Regulation is a specific addition to the GDPR, dealing with the confidentiality of communications and access to 'stuff on your devices' like cookies, IDs, etc. It was originally meant to enter into force at the same time as the GDPR but discussions are still ongoing between the EU institutions regarding the final text. At the time of writing, the final legislative text is expected to be adopted in the first half of 2019.

Both pieces of legislation are based on the Charter of Fundamental Rights of the EU of which the GDPR addresses the right to the protection of personal data (Article 8) while ePrivacy addresses Article 7 - Respect for private and personal life. The ePrivacy Regulation aims to bring, in particular, the use of different trackers into alignment with it. It's the overhaul of what used to be wrongly called the Cookie Directive.

Agencies can expect to see further changes on the horizon with the ePrivacy Regulation. For example, legitimate interests are likely not to be an option as a possible legal basis for lawful processing. It means that consent may constitute the primary means of assuring lawfulness of processing for targeted advertising in the future and appropriate tools/consent mechanisms need to be developed.

ACTION POINT
Prepare for the changes and develop tools for consumers to give consent.

5

WHAT ARE THE CONDITIONS FOR CONSENT?

The bar for valid consents has been raised much higher than before in the GDPR.[7]

According to the new text, consent must be 'freely given, specific, informed and unambiguous.'

The consent requirements include the following:

- The consent of individuals has to be proven by data controllers – and this needs to be made as transparent as possible from the outset.
- Organisations will need to ensure that consent is separated from matters such as terms and conditions so individuals have full clarity over what they are consenting to.
- Separate consents must be obtained for different processing activities.
- Organisations have to specifically name any third parties that they are sharing individuals' personal data with.
- Individual consent records need to be recorded and maintained – with as much detail as possible.
- Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
- Individuals should be easily able to withdraw their consent.
- Verifiable parental consent must be obtained for children aged 13-16. The exact age is specified by local transpositions of the GDPR. The current consensus is 13, aligning with US based COPPA with some exceptions.

ACTION POINT
If you market services or products that appeal particularly to children, put in place mechanisms to ask for and verify parental consent, adapting to local legislation.

ACTION POINT
Ensure that consumers can withdraw consent easily.

6

WHAT SHOULD I TELL CONSUMERS AND HOW?

Under the GDPR, the controllers have an obligation to provide more (detailed) information about data processing to consumers, or legally speaking, 'data subjects'. It has to be made available in 'a concise, transparent, intelligible and easily accessible form, using clear and plain language'. This is a challenge but also an opportunity for agencies to explore creative ways to build it into their work, as there is no definite format in which to provide the necessary information.

In their draft guidelines at the time of writing, the Article 29 Working Party - which at the moment consists of all the national data protection authorities and a representative of European the Commission and the European Data Protection Supervisor (EDPS) - gives the following requirements for information to be provided to consumers:

- Make sure that the information is understood by an average member of the intended audience by conducting periodic checks.
- Child addressees and other vulnerable members of society must be able to recognise that the information is being directed at them.
- It should be immediately apparent to the consumers where the information is.
- Avoid information fatigue.
- The information should be concrete and definitive. Language qualifiers such as 'may', 'might', 'some', 'often' and 'possible' should be avoided.
- Data controllers are free to choose the modality of providing information but where they have an online presence, an online layered privacy statement / notice is recommended. The first layer should contain information which has the most impact on the consumer and processing.
- There should be a reminder of the privacy statement / notice at appropriate intervals.

The list of information that has to be provided will expand.[8] The necessary information includes:

- The identity and contact details of the controller / their representative
- The contact details of the data protection officer
- The purposes and legal basis for the processing
- Where legitimate interests is the legal basis, the legitimate interests pursued by the controller / third party
- The recipients or categories of recipients of the personal data
- Details of transfers to third countries, the fact of same and the details of the relevant safeguards including the Commission's adequacy decisions and the means to obtain a copy of them or where they have been made available
- The storage period
- The rights of the consumer (to access, rectification, erasure, restriction on processing and objection to processing and portability)
- Where processing is based on consent, the right to withdraw consent at any time
- The right to lodge a complaint with a supervisory authority
- Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure
- The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source. The existence of automated decision-making including profiling, and if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the consumer

ACTION POINT

Develop a method to show information about data processing that satisfies all the GDPR requirements. Be crystal clear about:

- **Why are you collecting data?**
- **Who will use it?**
- **How will it be used?**

7

WILL PROFILING BE POSSIBLE?

You may need the consumer's explicit consent if you are making solely automated profiles of them, leading to decisions concerning them being made and producing legal effects or similarly significantly affecting them.[9] An alternative basis to assure the profiling is lawful is by entering into, or performing a contract between the data subject and the controller. It is currently uncertain how much targeted advertising there needs to be to necessitate consumers' explicit consent. However, the particular characteristics of online advertising and its possible consequences are likely to play a role. For example, if targeted advertising results in differential pricing barring someone from certain goods or services, an explicit consent might be needed.

Should an explicit consent be needed, more extensive measures should be taken compared to the conditions for normal consent, at least the right to obtain human intervention on the part of the controller to express his or her point of view and to contest the decision. Additional measures could include, for instance, consumers filling in electronic forms, sending emails or uploading scanned documents with their signatures.

ACTION POINT
Review your profiling practices and if necessary, develop new practices.

8

WHAT IF I TRANSFER DATA OUTSIDE OF EUROPE?

When data is transferred out of the European Economic Area, the first thing to check is whether there are agreements with this country about adequate levels of data protection by its domestic legislation or of the international commitments it has entered into.

It is important to think and ask where the data is stored to assure that the data subjects' rights are protected. Typically, 'in the cloud' is not a valid answer, as it's a server located somewhere.

Data transfers from the EU to the United States used to be valid under the 'Safe Harbor' framework which was declared invalid by the Court of Justice of the European Union in October 2015. Since then, the new 'Privacy Shield' has replaced the former framework and is at the time of writing still valid. Other options to assure that data transfers to the US are valid are standard contractual clauses for each data transfer – also called model contractual clauses - or Binding Corporate Rules (BCR).[10]

Note that as of the 29th of March 2019, due to Brexit, the UK might be considered a 'third country' for which adequacy will be required. Speculations as to which legal instrument might cover transfers from the rest of the European Economic Area to the UK are at the time of writing heating up. [11]

The best option probably remains to host data on the European soil, where Ireland is typically preferred or suggested as an option amongst other candidates such as Germany or even France.

ACTION POINT

If you transfer data outside of Europe, check for adequacy and be careful with onward transfers (i.e. transfers towards yet another country e.g. India). If there is no adequacy, use one of the following instruments: standard contractual clauses (also called model clauses) or binding corporate rules. For now, transfers from the EU to the US can also use the Privacy Shield.

9

HOW TO ENSURE THE SECURITY OF DATA PROCESSING?

Controllers are required to implement appropriate technical and organisational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing.[12] This includes the pseudonymisation and encryption of personal data. Organisations must have 'baked' data protection compliance into their data processing activities, collecting data only for specific purposes and processing the minimum amount of personal data necessary. Two specific points of data breaches and impact assessments are discussed below.

Data breaches

In order to ensure the security of data processing, agencies may need to be prepared to notify consumers of possible data breaches. The GDPR states that if your company has experienced a personal data breach and you are a controller, then you have an obligation to notify the supervisory authority within the next 72 hours.[13] Data processors need to notify the controller without undue delay after becoming aware of a personal data breach. They should then assess whether the breach is likely to result in a risk to the rights and freedoms of the consumer. If so, the data controller should inform consumers without the help of the processor, unless the contract between them states otherwise.

ACTION POINT

Move security (physical and technological) up from monitoring to alerting. Define how to register alerts internally and how to take action: which procedures will be required and who decides what to do within the procedures.

Data Protection Impact Assessments (DPIA)

Another way to align accountability obligations and ensure security of data processing is to undergo data protection impact assessments (DPIA). Note that they should be done prior to the processing of personal data. A DPIA is mandatory when the data processing is likely to result in a 'high risk'. It is likely to apply to digital analytics, data management platforms and customer data platforms.

The Article 29 Working Party, which at the moment consists of all the national data protection authorities and a representative of European the Commission and the European Data Protection Supervisor (EDPS), has issued guidance on the topic. Their elaborated criteria when a DPIA should be undertaken can be found in the Annex.[14] If at least two points in this criteria are met, the processing is considered to be 'likely high risk' and only thoroughly documenting reasons for not carrying out a DPIA can be considered as enough of a reason not to carry out one.

Processing operations may be grouped for a single assessment where similar technology is used to collect the same sort of data for the same purposes. The national data protection authorities (supervisory authorities under the GDPR) will in due course establish their own lists of the processing operations that require a DPIA.

The data controller - who determines the purposes and means of the processing of personal data - is responsible to ensure that the DPIA is carried out with the advice of the Data Protection Officer. If the processing is wholly or partially performed by a data processor - i.e. an agency processing data on behalf of the controller - , it should assist the controller in carrying out the DPIA and provide any necessary information.

Data controllers are free to choose a DPIA methodology that fits them as long as the minimum features of a DPIA are documented. [15]

ACTION POINT
Make sure DPIAs are carried out as necessary or ask clients to minimise risk.

10

HOW TO MANAGE THE DIFFERENT CONSUMER RIGHTS?

As consumers, or legally speaking, data subjects, are gaining more rights, you also have to be careful with the data you are already in possession of. Agencies will need to put in place clear processes to be able to respond to consumers' requests about their personal data. The rights, some of which have already been discussed in this report, are listed below:

- Right of access by the data subject[16]
- Right to rectification[17]
- Right to erasure ("right to be forgotten")[18]
- Right to restriction of processing[19]
- Notification obligation regarding rectification or erasure of personal data or restriction of processing[20]
- Right to data portability[21]
- Right to object[22]
- Automated individual decision-making, including profiling[23]

Adhering to these requirements depends upon recognition of the compliance obligation (by your clients) and linkability of data. A lot of the data is being linked between different tools and application program interfaces. It should be decoupled - making sure that it does not, for example, pass through from audience measuring to ad targeting. The delinking should be possible and correctly reflected in the contract, unless the vendors accept to become joint controllers.

Please note that acting on the consumers' requests is subject to other obligations of the data controllers and processors. It is possible that you may have an obligation to keep certain data for the state. Make sure to communicate this with your clients.

ACTION POINT

Ensure that you have internal procedures in place to respond to consumers' requests about their personal data and that you have kept records of the processing which can be transported, edited and deleted if necessary.

11

WHAT RECORDS TO KEEP?

For controllers:[24]

- the name and contact details of the controllers, their representatives and the data protection officer
- the purposes of the processing
- a description of the categories of data subjects and of the categories of personal data
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
- transfers of personal data to a third country or an international organisation, their identification and the documentation of suitable safeguards
- the envisaged time limits for erasure of the different categories of data
- a general description of the technical and organisational security measures

For processors:[25]

- the name and contact details of the processors and of each controller on behalf of which the processor is acting, their representatives and the data protection officer
- the categories of processing carried out on behalf of each controller
- transfers of personal data to a third country or an international organisation, their identification and the documentation of suitable safeguards

Controllers are also required to keep a record of all the data breaches.[26]

The information should be in writing, including in electronic format.

The records should be available to the supervisory authority upon request and provided to consumers. There are derogations for smaller companies, less than 250 employees; data processing is occasional, etc. However, they will not apply where sensitive data are processed.

Tip:
Template by Belgian DPA/Supervisory Authority, translated into English

12

HOW TO MONITOR COMPLIANCE WITH THE GDPR?

Data Protection Officer

As a result of the GDPR, some controllers and processors will be required to appoint a dedicated Data Protection Officer (DPO) to assist their organisations to monitor internal compliance with the GDPR. It is necessary 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'.[27]

In the Article 29 Working Party's guidance, companies that process data for online behavioural advertising are specifically identified as companies which would need to appoint a DPO.

Even if your client has a DPO and you use data provided by the client, you may need to have your own DPO if both of you process data on a large scale. It is possible for a group of undertakings to designate a single DPO provided that he or she is 'easily accessible from each establishment' and 'in a position to communicate efficiently with consumers and co-operate with the supervisory authorities concerned'.[28] This also means that this communication must take place in the language or languages used by the supervisory authorities and the consumers concerned. If your Group is doing business across Europe, you might want to consider appointing several DPOs.

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. DPOs should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have sufficient understanding of the processing operations carried out, as well as the information systems and data security and data protection needs of the controller.

The Data Protection Authorities (Supervisory Authorities under the GDPR) list things that an organisation should ensure for the DPO, listed in the Annex.[29]

DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law. The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks.

Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interest. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

ACTION POINT
Assess whether you need to appoint a DPO.

Codes of conduct, seals, certificates and standards

Certain companies are only willing to work with other providers if they have certificates or seals in place or adhere to certain standards. These can be useful in terms of best practices.

The Article 29 Working Party will publish guidelines on this point in due course.

Seals and certificates are encouraged in the GDPR, as they were in the directive. Due to the accountability principle, data controllers typically want to make sure their choice of data processors is aligned with their obligations. As such, they have a duty of due diligence, which could translate into an audit. Standards, seals and certificates are mechanisms to ensure data protection obligations under the GDPR are understood and processes set in place to align with such obligations.

While certificates vary possibly per region and sector, some best practices can be found within existing standards. Typically, the ISO/IEC 27000 family of standards is a starting point for security best practices in the form of codes of conduct.

The question often arises with respect to which seals and/or certifications are required. This is a matter of market influence as well as recognition yet agencies would be advised to explore the topic in order to assure their data processing operations can assure a level of confidentiality, integration and availability before moving possibly beyond to explore regional or sectorial best practices.

13

OPPORTUNITY OR CHALLENGE?

The way agencies are set up, each department may have their own incentives. This may not work towards minimising risks towards the entire company. Employees of all levels should understand the obligations and training that is needed. Only appointing a Data Protection Officer will be enough to assure that the accountability principle is respected.

- Overall, the legislative changes should create better, deeper, more respectful customer relationships for advertisers and publishers. This will be an opportunity to build greater consumer trust, supporting data quality.
- Agencies will need to consider a 'What's in it for me?' strategy - provide value exchange and ask consumers what they want and review whether marketing communications offer relevance and value.
- Industry players focusing on best practice should benefit from the GDPR, albeit it is hard work in the short-term.
- You must get organised now, identify required changes and create a roadmap to compliance by May 2018 and beyond.
- Your incentives might be skewed, make sure you support accountability & minimise risk for your company!

If you have any questions or comments about this Report, please contact the EACA team:

info@eaca.eu

Dominic Lyle
EACA Director General
dominic.lyle@eaca.eu

Sofia Karttunen
European Affairs Officer
sofia.karttunen@eaca.eu

ANNEX

Legislative texts:

The current Data Protection Directive 95/46/EC

The new General Data Protection Regulation 2016/679

The current ePrivacy Directive 2002/58/EC

The Commission's proposal and the position of the European Parliament for the new ePrivacy Regulation

[1]Art. 4 (7) of the GDPR
[2]Art. 4 (8) of the GDPR

[3]Controller: Art. 25

- Must implement appropriate technical and organisational measures in an effective manner and to integrate the necessary safeguards into the processing
- Develop pseudonymisation techniques and ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed

Processor: Art. 28

- Where a processor carries out processing on behalf of a controller, they must provide sufficient guarantees to implement appropriate technical and organisational measures
- The processor shall not engage another processor without prior written authorisation of the controller
- Processing by a processor shall be governed by a binding contract between them and the controller (conditions of which are listed in Article 28)

Joint-Controller: Art. 26

- Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance, for example, in providing information to consumers
- Irrespective of what the arrangement of responsibilities between the joint controllers is, consumers may exercise their rights against each of the controllers

[4]Article 6
[5]Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Tehcniques.

[6]Future of Privacy Forum, Visual guide to practical data de-identification.

[7]Article 7
[8]Articles 13 - 14
[9]Article 22

[10]European Commission, Model contracts for the transfer of personal data to third countries.

[11]European Commission, Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection.
[12]Article 32

[13]Articles 33- 34

[14]Evaluation or scoring
- Includes building behavioural or marketing profiles based on usage or navigation on a website

Automated decision-making with legal or similar significant effect
- Processing that aims at taking decisions on data subjects that may lead to exclusion or discrimination against individuals

Systematic monitoring
- Where personal data may be collected systematically in publicly accessible spaces

Sensitive data
- Collecting special categories of data such as political opinions and criminal convictions

Data processed on a large scale
- Things to take into account: the number of data subjects concerned, the volume of data, the duration of the data processing activity and its geographical extent

Datasets that have been matched or combined
- Data originating from two or more data processing operations exceeding the reasonable expectations of the data subject

Data concerning vulnerable data subjects
- Individual is unable to consent to, or oppose, the processing of his/her data

Innovative use or applying technological or organisational solutions
- Such as combining use of finger print and face recognition for physical access control

Data transfer across borders outside the European Union
- Actual transfers and the possibility of further transfers

When the processing in itself prevents data subjects from exercising a right or using a service or a contract

[15]Article 35(7)
[16]Article 15
[17]Article 16
[18]Article 17
[19]Article 18
[20]Article 19
[21]Article 20
[22]Article 21
[23]Article 22
[24]Article 30.1(a) - (g)
[25]Article 30.2(a) – (d)
[26]Article 33(5)
[27]Article 37(1)(b)
[28]Article 37(2)

[29]
- The DPO is invited to participate regularly in meetings of senior and middle management.
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must always be given due weight. In case of disagreement, the DPAs recommend, as good practice, to document the reasons for not following the DPO's advice.
- The DPO must be promptly consulted once a data breach or another incident has occurred.
- There must be active support of the DPO's function by senior management (such as at board level).
- There must be official communication of the designation of the DPO to all staff to ensure that their existence and function is known within the organisation.

GDPR Essentials for Marketers Online Training

To complement these guidelines, EACA offers an online course in association with Econsultancy to get to grips with the GDPR before it comes into force in May 2018.

The online course is split across three themes: the law as it stands today - and as it will be, what the changes mean for organisations, and the implications for each channel or activity within marketing.

Each section brings the topic to life and clarifies grey areas through seven video modules with reading lists and 'test your knowledge' quizzes.

The key learning objectives are:

- The letter of the law: what the relevant laws already contain, and the specific new provisions of the GDPR
- Key principles and what they mean (implications, risks and costs)
- What needs to be done differently in each of your core marketing activities
- Practical tips for the top actions you need to take
- Specific implications for each marketing channel

The course is delivered completely online and takes about 14 hours to complete. It's designed for you to study at your own pace with 30-days access to the course content. Bookings are open as of the beginning of February, with the first course date on 27 February and the second on 27 March 2018. Upon completion, participants will receive an Econsultancy certificate of completion displaying their 14-hours of CPD credits.

The course is designed for anyone wishing to learn more about the GDPR; especially Marketing Directors, Agency Heads and Senior Executives, Data Team Leaders, App developers, Marketing Managers and Data Marketing Managers.

The course costs EUR €695.00. EACA members will receive a 10% discount by using the code: **EACAGDPR10**. To book your place, please click here. For more information, visit our website. For any questions or concerns, please contact us at inspire@eaca.eu.

EUROPEAN ASSOCIATION OF
COMMUNICATIONS AGENCIES

info@eaca.eu

www.eaca.eu

@EACA_eu

152 bd. Brand Whitlock,
1200, Brussels