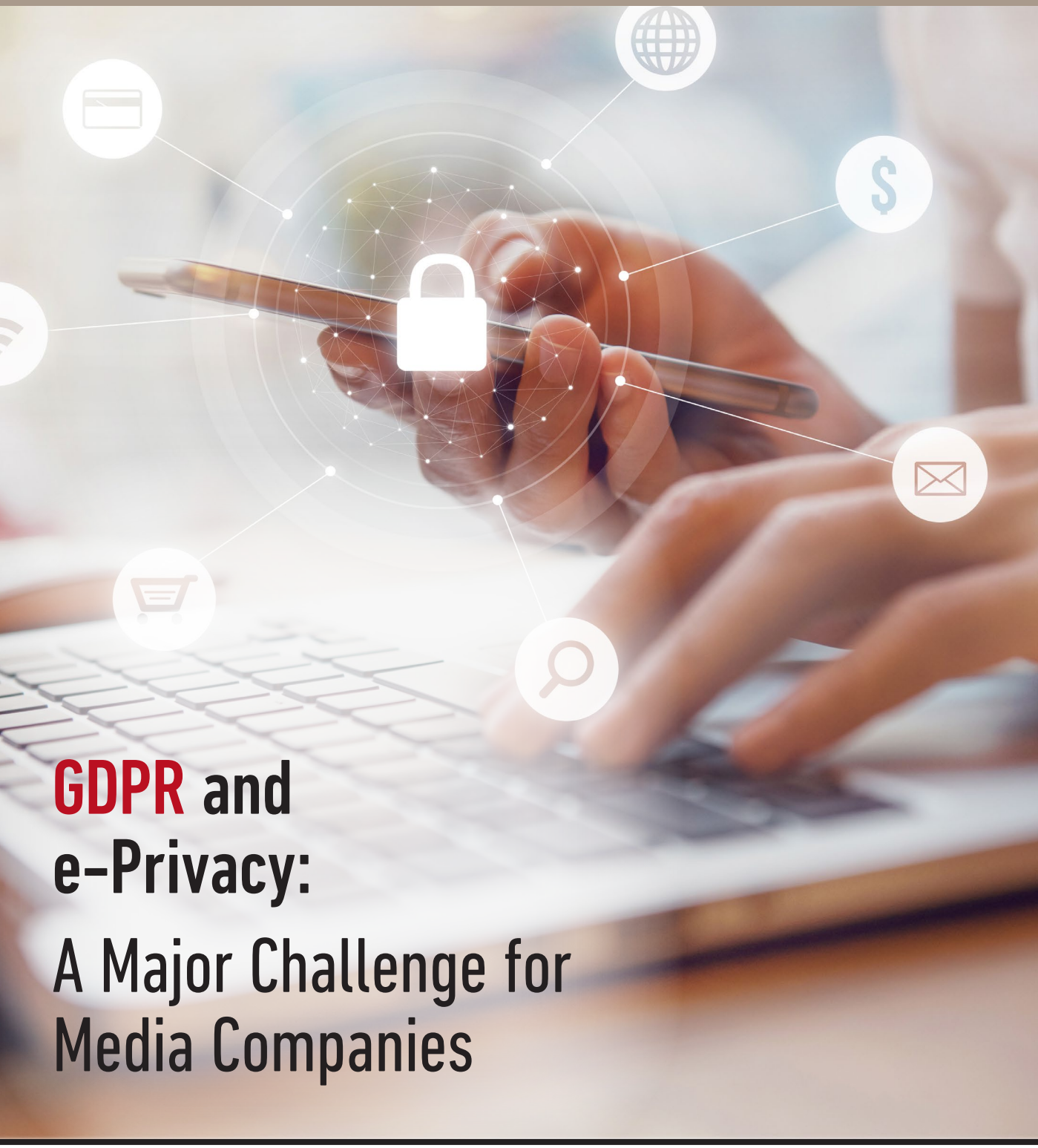


GDPR and e-Privacy:

A Major Challenge for Media Companies

BAROMETER
MEDIA2017
NUMBER | 5

MAZARS

MAZARS IS AN INTERNATIONAL, INTEGRATED AND INDEPENDENT ORGANIZATION, SPECIALIZING IN AUDIT, ADVISORY, ACCOUNTING, TAX AND LEGAL SERVICES. ON 1 JANUARY 2018, MAZARS WAS OPERATING IN 86 COUNTRIES FORMING ITS INTEGRATED INTERNATIONAL PARTNERSHIP. MAZARS DRAWS ON THE EXPERTISE OF 20,000 PROFESSIONALS. LED BY 980 PARTNERS, THEY ASSIST MAJOR INTERNATIONAL GROUPS, SMES, PRIVATE INVESTORS, START-UPS AND PUBLIC BODIES AT EVERYSTAGE IN THEIR DEVELOPMENT.

CONTENTS

KEY **FINDINGS**

MEDIA COMPANIES ARE PARTICULARLY CONCERNED BY THE GDPR AND E-PRIVACY REGULATIONS

In a context of increased digital activity, media companies collect a considerable quantity of personal data. This data enables them to offer better-targeted opportunities for advertisers.

This makes targeted advertising, based on data collected from users, one of the main opportunities for media companies to boost their digital revenue.

Parallel to this, new legislation has been introduced governing the use of personal data. These new EU regulations, the **General Data Protection Regulation** and the ***e-Privacy Regulation Project,*** are of national and international scope and aimed at making companies responsible for protecting personal data. Adjusting practice to comply with these new regulations within the binding timetable imposed is a key challenge for media companies.

INTRODUCTION

Each year, Mazars' Media & Information Group analyzes the risk factors outlined in the annual reports of the top 100 media companies (in Europe and the USA).

Last year, the risk of **data loss and hacking** was the leading concern and therefore led to a barometer dedicated to the risk of cybercrime.

This study specifically highlighted differences in awareness of the risk of data loss between the USA and Europe. Whereas US companies appeared highly aware of the importance of data security, European companies seemed less concerned by this issue, notably due to less strict regulations.

This absence of strict regulation ended on April 27th, 2016 with publication of the General Data Protection Regulation (GDPR) by the European Commission. This regulation is aimed at making companies responsible for protecting personal data.

Whether on a legal, organisational or technical level, the amount of work involved in compliance is considerable for all companies and the regulation will be coming into force on May 25th, 2018.

This year, Mazars is therefore dedicating a barometer to the GDPR, focusing on the issues specific to media companies, to help you meet the challenge of compliance with the new regulations.

A risk factor analysis performed using reference documents available in 2017 reveals the following concerns for media companies:

Risk factors	3-year variation
Risk of data loss and hacking (cybercrime)	+ 8 points
Risk of asset depreciation	+ 4 points
Risk of failure of group strategy implementation and merger-acquisition operations	+ 3 points
Social and environmental risks	+ 2 points
Risk of dependence on third parties	+ 1 point
Risk regarding regulations and legislation	+ 1 point
Risk relating to insurance policy	+ 1 point
Risk relating to international operations	+ 0 point
Risk relating to seasonal business and stock market fluctuations	+ 0 point
Risk relating to reputation	- 1 point
Risk relating specifically to the media economy	- 1 point
Financial risk	- 1 point
Risk of mistaken anticipation of consumer demand	- 1 point
Risk relating to legal disputes and proceedings	- 2 points
Risk relating to intellectual property	- 2 points
Risk relating to funding pensions	- 2 points
Risk relating to competition and mergers in the media industry	- 3 points
Risk relating to attracting and keeping key employees	- 3 points
Risk relating to the economy as a whole	- 4 points

1 WHAT IS THE GDPR?

The General Data Protection Regulation

The GDPR is the **regulation** that guarantees **individuals** that **use** of digital (and other) data concerning them is **processed, used, disseminated** and kept in a **transparent** manner, and that the entities processing this data will not perform any actions without the individuals concerned having first **agreed** or been **notified** of the **processing** applied to their data.

In practice, this involves:

> The right for individuals to be **informed** of all processing applied to their data

> An obligation for the entity using the personal data to **restrict** the **gathering** and **use** of data solely **for the purposes** of processing as set out and provided for **information** to the individual concerned

> The right for individuals to **know** what personal data the entity holds and **how** it intends to use it

> The right for individuals to **move,** and not simply duplicate, their personal data from one organization to another – **the principle of data portability**

> The right for individuals to request the **deletion** of data held by an entity which no longer uses or needs it – **the principle of the right to be forgotten**

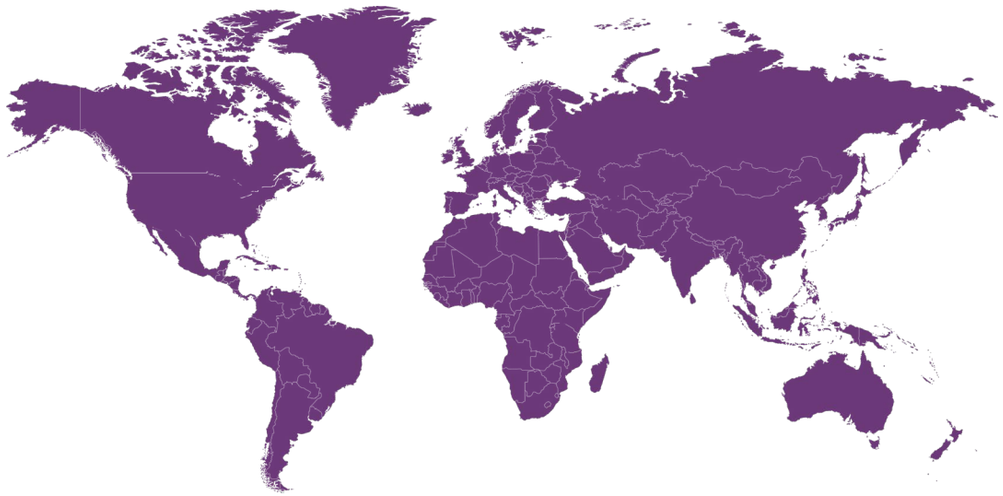
> The appointment of a ***Data Privacy Officer*** in organizations meeting certain criteria

> Companies that gather data must **ensure compliant processing of said data by their subcontractors or partners**

> In the event of personal data breaches, **an obligation to notify the appropriate supervisory body within 72 hours**, and the obligation to communicate the data breach to the data subject without undue delay if it is likely to result in a high risk

WHAT ABOUT **NON-EU ORGANIZATIONS**?

Throughout the world, data privacy has become an issue and a major topic for companies, but only the European Parliament passed the official GDPR law. Indeed, unlike in some other countries, European citizens consider privacy differently: it has always been a basic human right. Despite this cultural distinction, and although the subject is not as well implemented in non-EU companies' DNAs, these cross-cultural differences should be seen as an opportunity for international organizations to take a deeper look at user privacy. By preparing for and complying with the new regulation, international organizations will see that there are real opportunities as well.



IS MY ORGANIZATION CONCERNED?

This law does not only impact European organizations. Any organization that uses personal data of persons residing in the EU to provide services, sell goods, or monitor their behavior, will be impacted. For instance, a US-based newspaper that has German readers will be expected to comply with the GDPR as it tracks, collects, stores, and uses data from this European person.

WHAT ARE THE OPPORTUNITIES?

The GDPR represents an opportunity for international companies, mainly to:

> Transform and improve your current approach to data privacy

> Leverage the value of your data by improving the way you track, collect, store, and use it

> Ensure that your organization is ready for tomorrow's global digital economy

IS IT TOO LATE TO COMPLY?

Although the May 2018 deadline is approaching, the majority of organizations will not be fully compliant. Until now, due to the complexity of this regulation, the "wait and see" attitude was the norm. However, as some benchmarks are available and good practices are in place, now is the time to react. GDPR regulators expect to see plans in place.

For a non-EU company, complying with an EU regulation can be challenging. Mazars, an international group with its roots in Europe, with deep knowledge around data privacy and European Law, can guide non-EU companies to ensure a successful transition to GDPR compliance.

The GDPR involves at least **four separate, yet interwoven subjects** that render its application relatively complex, requiring in-depth consideration prior to any action.

NOTE

Addressing only one of these subjects would constitute a risk and potentially expose the organization to a fine.

2 THE MEDIA, A SECTOR PARTICULARLY CONCERNED BY THE GDPR AND E-PRIVACY

In an increasingly digitalised industry, the processing of personal data is a lever for creating added value.

Media digitalisation and monetizing content

Over the last 20 years, arrival of the Internet has forced the media industry to reinvent its business model and adjust to the consequences of digitalisation of media content.

Whereas media companies used to control distribution of their content, user behaviour has undergone profound and lasting changes:

> **Predominance of free content,** although this trend is beginning to abate as consumers are becoming used to paying for premium content

> Consumer demand for the option of consulting **content on multiple platforms**

> Increasing demand for a **consumer experience** including interactivity, on-demand distribution and unlimited available content

To meet these demands, the media industry has had to rebuild its customer relations, fragmented by the diversity of existing platforms and devices, and monetize content that has become wholly or partially digital.

Digital content is principally monetized by **subscription revenue** or **advertising revenue.**

Subscriptions

Subscriptions are sometimes mandatory for accessing content, but can also take the form of paywalls, which grant visitors a free trial period, consisting of a specific number of pages, views or audio files, before blocking further access without subscription or payment.

SPOTLIGHT ON THE PRESS

According to Google, customer satisfaction drops when a paywall appears more than once in every ten consulted articles. This led to Google abandoning its First Click Free program offering news providers better visibility on its search engine in exchange for three free articles a day. The new rule now provides for:

> Between 6 and 10 free articles

> Systematic indication of content subject to a paywall

Subscription is the most stable form of monetization for media companies, who are then guaranteed a loyal audience.

However, across all countries, only one in ten (13%) pay for online news, though some regions (Nordics) are doing much better than others (Southern Europe and much of Asia), per the Digital News Report 2017 from Reuters Institute.

« Even though studies show that the public are becoming more used to paying to access information, the sometimes laborious process of subscribing can act as a deterrent.

This is not good for users or press publishers, for whom subscriptions are an increasing source of revenue."

Google official blog - October 2017.

To compensate for difficulties in increasing subscriptions and monetizing their content, media companies are gat-hering ever more personal data on users to boost their revenue by offering ad-vertisers better-targeted ad-vertising opportunities.

THE GAT HERING OF PER SONAL DA TA

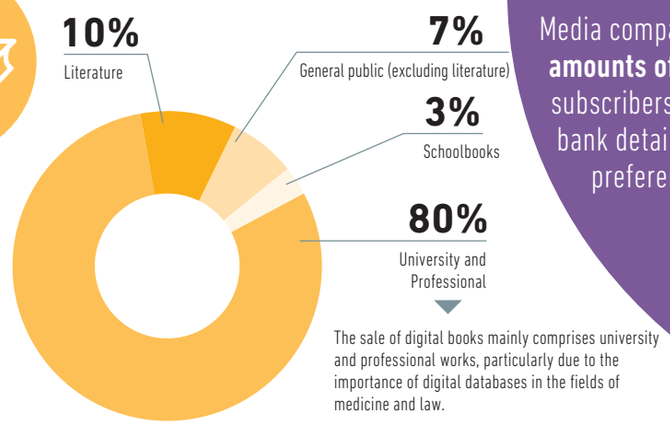
Media companies gather **considerable amounts of personal data** from their subscribers; not only their names and bank details, but also their consumer preferences and frequency of use.

In this context, monetising data has become a key issue in compensating for the difficulty in generating revenue from subscriptions

The press has long been the media most affected by the breakthrough of digital technology and has rapidly adjusted its business model, notably through the introduction of online subscription, leading to the possibility of gathering personal data, including names, addresses and bank details. In addition, reader behaviour and traceability generates precious information in the global monetisation of content.

MAIN SOURCE OF NEWS BY AGE - ALL MARKETS

*Source: Reuters Institute 2017



The sale of digital books mainly comprises university and professional works, particularly due to the importance of digital databases in the fields of medicine and law.

The **book** sector, which has been far less affected by digitisation than the written press, is now offering unlimited content in exchange for subscription, for example with Amazon Unlimited. Distributors of digital books can now track the behaviour of their readers and gather a significant amount of information, such as the number of pages read, speed of reading, underlined sections of text, time spent on reading a page, reading hours and the location of readers.

The **music** industry has been revitalized by subscriptions to streaming offered by companies such as Deezer, Apple Music and Spotify.

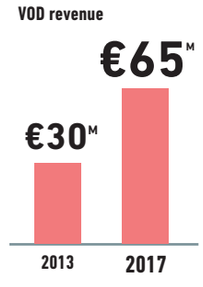
Market leader Spotify has added 20 million extra paying subscribers over the last 12 months and Apple Music, around 10 million.

Continuing this trend, at the beginning of 2017, the US online radio service Pandora launched its paying streaming service to earn revenue from its pool of 81 million monthly listeners. Knowledge of user preferences enables music streaming sites to advertise the tour dates of favourite artists and make suggestions for listening based on their preferences to users of affiliated streaming sites.

+5%
Growth in 2016

€ 1.3 billion euros
Industry revenue
(3 times less than in 2002)

*Source: IFPI SNEP, French Syndicate of Music Producers



70%
Of online traffic comprises video streaming

The **audiovisual** sector is also increasingly affected by video on demand or by more global offers provided by players such as Netflix. Yet traditional actors also continue with their transformation, e.g. developing new platforms and better integration of digital extensions in the content creation process. In September 2017, due to the massive expansion of audiovisual streaming, Google and the French broadcasting piracy protection association (ALPA) signed a partnership to combat audiovisual piracy together. In addition, Google has undertaken to implement the necessary resources to prevent the purchase of fraudulent keywords on its Adwords service for illegal streaming sites.

Advertising revenue

Due to the difficulty in generating revenue from subscriptions, Internet monetisation has traditionally been developed by advertising, mainly in the following forms:

> Display, which consists of displaying advertisements in the form of images or videos visible on the webpages delivering the content

> Content sponsored by third parties, such as articles and partnerships

> Interstitial advertising on smart phones and tablets

Over the years however, technological multi-screen developments and audience fragmentation have created a challenge for broadcasters seeking to monetize their audiences in an advertising market where revenue is stable, with growth at around 0.1% in the first half of 2017, according to the IREP.

Moreover, Google and Facebook represent over 50% of the advertising market in 2017, with Amazon, although still small in terms of market share, growing faster than both of them.

To rival big players such as Google, Apple, Facebook and Amazon, digital players, including a significant number of media companies, have created alliances to pool their data to improve advertising targeting.

Most of these platforms mainly operate via the use of cookies, on fixed or mobile devices, to boost performance in programmatic advertising.

As cookies, IPs, user preferences, and web navigation history are considered personal data, the main challenge for a media player will be to comply with the GDPR while still optimizing user targeting. Ultimately, within this new regulatory context, revenue generation through advertisement and the improvement of the user experience will be a complex balance to reach.

| DID YOU KNOW?

Around 30 European media companies sent an open letter to the European Parliament to protest against restrictions on the gathering of data imposed by the EU. In this letter, they explain that "e-Privacy deprives publishers of the capacity to inform their readers of the reasons why their consent is sought, explain the benefits of editorial content and customized marketing and remind them of the importance of subscriptions and advertising in the economic model of a quality press".

KEY INFO

The media industry is characterised by a business model that is making increasing use of its users' personal data. As such, media companies are implementing strategies to extend the nature and type of collected data. The GDPR requires the holders of personal data to guarantee the security of their data: confidentiality is one of the key aspects of the legislation. To restrict unauthorised use of profiling, the EU legislator has drawn up another regulation to protect privacy online, the e-Privacy regulation project, which will come into force soon. EU legislation stipulates that cookies can be considered personal data. However, the legislation only concerns cookies used to profile users.

To comply with legislation, media companies must clearly inform users of the exact purpose of their cookies. Furthermore, companies will not be able to place cookies on users' computers without explicitly obtaining their consent, by means of "affirmative action". A simple statement that the website uses cookies is no longer acceptable under the new regulations.

More generally, in light of the considerable amount of personal data processed by media companies, the key challenge lies in implementing an organisation capable of:

> Identifying and tracking collected data

> Restoring this personal data to a specific user

> Ensuring their many partners also comply with EU regulations

The legislator has provided for fines of up to 4% **of global annual revenue** or **20 million euros** (whichever is higher), for breaches to either the GDPR or the e-Privacy regulations.

3 WHAT DOES THIS CHANGE?

The GDPR applies to the 28 EU member countries and replaces legislation previously in force concerning the protection of personal data.

From declarations to compliance

CNIL rules amounted to an obligation to provide declarations to the French Data Protection Authority (CNIL). The GDPR, on the other hand, requires a **compliance procedure** that companies will need to implement. It is therefore up to the senior management of companies to take up the issue and draw up a **wide-ranging corporate plan**.

Implementing a procedure and organization

Whenever there is a burden of compliance, an organization must be set up not only to perform the task of compliance, but also to ensure the procedure continues to function over time. This organization normally involves the appointment of a Data Privacy Officer (DPO), who can act as a useful pivot, even for companies that do not meet the criteria imposed by the regulation.

In all cases, companies must also appoint one or more "processing managers", tasked with drawing up the purposes and methods of processing personal data within the company. Data is deemed to be personal when it relates to an individual that is directly or indirectly identified or identifiable.

Lastly, over and beyond the appointment of managers, companies must ensure compliance by introducing a process that enables them to meet the requirements of the regulation as regards the identification and location of personal data, as well as how it is processed, kept, deleted and accessed.

"Many US companies are just starting to realize the breadth and depth of impact that GDPR will have on their business and IT operations. It is forcing them to establish not only a better and more formalized understanding of the mapping of personal data on their business processes and IT infrastructure, but also to have a clearer understanding of their relationships and responsibilities with third parties with which they share personal data. Because it makes more sense for most of these organizations to implement the GDPR principles and data subject rights for all personal data regardless of nationality or citizenship, the end result will be increased personal data privacy and rights for many non-EU residents."

Brian Browne,
Principal at Mazars USA, Cyber Risk

"GDPR and eprivacy regulation are massively disrupting the technology and media industries. Some organizations will have to modify their business model for a simple question of survival. For consumers, this could mean the end of free media as these companies will not be able to push ads the same way. On the other hand, it is a tremendous opportunity to bring back the individual at the center of the relationship by pushing innovation, e.g. around data portability and consent management. There is no doubt that the GAFAs will lead the way."

Nicolas Quairel,
Global Head of Technology & Digital Solutions,
Mazars UK

4 WHAT NEEDS TO BE DONE?

3 STEPS TO COMPLIANCE

| NOTE

Compliance with the GDPR and e-Privacy regulations is a dense and complex process that will inevitably take time to implement. Media companies gather a significant amount of data from different sources and now need to make preparations to be able to trace this data and restore it if necessary.

1 PERFORM AN AUDIT

The GDPR and e-Privacy regulations impose many new obligations. Firstly, before implementing any new organisation or process, companies need to **map**, **identify** and **list** the areas in which they diverge from the regulation requirements, in order to focus their efforts on the subjects that call for the greatest or most urgent adjustments.

Companies need to take stock of where personal data is hosted within the company, together with how it is processed, kept, used and consulted, in order to commence a compliance procedure.

This audit comprises two separate phases:

> Mapping processes listed in a special register

> Setting out and prioritizing corrective actions

2 GET PREPARED TO MEET THE VARIOUS REQUIREMENTS OF THE EU REGULATIONS

The regulations are highly precise and the CNIL has produced various guides and recommendations. Companies should follow these recommendations to ensure they explicitly comply with the full set of obligations stipulated by the legislation. In other countries, local regulators should be implementing similar principles. This preparation involves:

> **Appointing a coordinator, the DPO**

> **Drawing up and integrating internal procedures** relating to the GDPR and e-Privacy within the company

> Formally **documenting a certain number of subjects** and reviewing the contracts of undertakings that include services processing personal data

3 INTEGRATE GDPR AND FUTURE E-PRIVACY REQUIREMENTS INTO PROJECT DESIGN – *PRIVACY BY DESIGN* AND MANAGE THE RISKS

Leading on from the previous point, as there are many obligations in the regulation, companies must ensure these form an integral part of project design from the start, especially with respect to IT projects. This is referred to as ***privacy by design***, which aims to ensure that GDPR is an integral, native part of all corporate projects.

1 PERFORM AN AUDIT

Mapping processes listed in a special register

This phase should enable the entity **to identify** and **qualify** all types of **personal data** to which it may have **direct** or **indirect** access.

For this purpose, for each "batch" of data identified, it must:

> **Establish** what **processing** is applied

> **Qualify** the **type** of personal data

> **Qualify** the **objectives** sought by processing the data

> **Identify** the **persons** capable of processing this data

> **Identify** the **datafeed** and pathways that track this data

In addition to these tasks identifying and qualifying the data, for each batch, the entity should **appoint** a **processing manager** and **enter** the information relating to this data in **records of processing activities.**

This register will be used to collect other information, such as data preservation time, security measures implemented and the data storage location.

Identifying and prioritizing corrective actions

The second project phase involves **measuring any divergences** that may exist between the information gathered and listed in the processing registers and the **regulatory requirements.**

Special vigilance is required in the case of:

> **Free-access** data or data with **no technical protection**

> Personal data that reveals **social or ethnic origins**, **gender** or **political orientations,** genetic or biometric information or criminal records

> Data destined to be **sent** to **countries** deemed **unreliable** in protecting personal data or to potentially non-compliant third parties

> Decisions with legal effects taken by the entity based solely on the computer processing of data (e.g. profiling)

TASKS

- ✓ **For each item in the register, specify the degree of risk as regards divergence between reality and obligations**
- ✓ **Draw up an action plan for the entity and its external partners (particularly subcontractors)**

2 GET PREPARED TO MEET THE VARIOUS REQUIREMENTS OF THE UPCOMING EU REGULATIONS

Appointing a DPO

Over and above identifying the data, processing and divergences with respect to the standard, the regulation calls for a **permanent**, **dedicated** organization to be created within the entity.

This organization requires various components, whether compulsory or not in the regulation.

The regulation provides for the appointment of a coordinator within the entity, tasked permanently with ensuring **compliance with** the **regulation.** This person will become the **DPO,** ***Data Privacy Officer.***

The role of the coordinator is to **advise** and **orchestrate:**

> Informing and advising processing managers, **subcontractors,** and the **senior management** of the entity

> **Advising** the organisation on the processing to be applied to personal data with respect to all components of the regulation

> **Acting as an interface** with the supervisory body (CNIL) and cooperating therewith

Establishing and integrating internal processes relating to the GDPR in the entity

The processes implemented must ensure compliance with rules regarding:

> The protection of personal data as soon as any application or processing is implemented – *privacy by design*

> **Information,** by raising awareness and **training** employees within the entity in personal data issues

> The **practical handling** of **claims** as provided for by the regulation **– access, rectification, portability, oblivion**

> The **information** of people concerned in the event of a **breach** of personal data or the occurrence of an **incident**

Formally documenting a certain number of subjects

A key component of this regulation involves **documentation of the mechanism** via:

> **Formalizing procedures**

> The **processing register**

> Drafting **clauses** in **contracts** with subcontractors or suppliers

> **Documenting risk studies**, whether prior to implementing processing on application, or following a risk audit

> **Documentation** drafted for **persons** concerned for **information purposes**, as well as for obtaining **consent**

NOTE

Appointment of a DPO is only mandatory in specific cases: a public body or a body whose purpose it is to mass-process data deemed to be sensitive, or in cases of systematic monitoring of data.

However, the CNIL strongly recommends that all organisations have such expertise at their disposal.

3 INTEGRATE GDPR AND *E-PRIVACY* INTO PROJECT DESIGN – *PRIVACY BY DESIGN* AND MANAGE THE RISKS

A **risk management** or ***Privacy Impact Assessment (PIA)*** must be performed on two occasions:

> When **introducing** processing or an application using personal data

> As soon as a **divergence** is **revealed** between obligations relating to the regulations and reality within the entity

This means that for all processing or applications capable of processing personal data, entities must:

> **Describe** the **processing** and its **purposes**

> Assess the data strictly required for the processing

> Evaluate the risks linked with compliance with data privacy for those concerned

> Set out the measures to be taken to circumvent these risks

NOTE

The GDPR and e-Privacy are complex upcoming regulations that require risk management for all applications or processing of personal data.

Media companies that process a significant amount of data must also ensure they implement appropriate safeguards.

4 IMPLEMENTATION SCHEDULE

THE MEDIA & INFORMATION GROUP

The Mazars Media & Information Group brings together experienced professionals with focused industry expertise in the media sector. We provide tailored audit, tax and advisory services to a range of clients, from young companies to international media groups.

Our experience working with key players in this sector enables us to provide you with the expertise you require to meet the major challenges facing the media industry. For more information on the Media & Information Group, visit: www.mazars.com

INFORMATION SYSTEM SECURITY & *DATA PRIVACY*

The computerisation of all economic activity is now a reality in the business world. Delinquents have adapted to this situation and are now using this "hyper connection" to infiltrate systems and use them either directly or to steal information contained therein and use it for the purposes of traditional fraud.

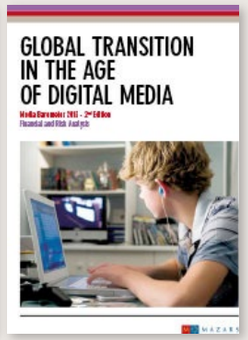
Mazars experts provide tailored cyber-security services, including: **intrusion tests, assistance with security contracting in major projects, assistance with security governance, investigation following suspected fraud or security incidents**. Mazars experts provide support in evaluating the security level of your information systems and propose operational / organisational corrections wherever necessary. For more information concerning our information system security & *data privacy offers*, go to our website: www.mazars.com

OUR PUBLICATIONS

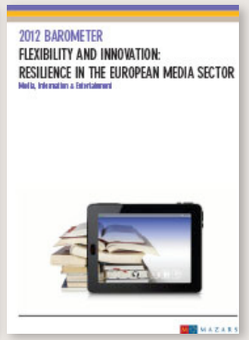
2015

2014

2013



2012



For more information:
www.mazars.com

Praxity
MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS

MAZARS