INTERGRAF
European Federation for Print and Digital Communication

INTERGRAF GUIDE TO THE EUROPEAN DATA PROTECTION REGULATION FOR EUROPEAN PRINTERS

December 2016

"European printers need to start taking steps now to ensure they will be compliant with the General Data Protection Regulation in May 2018.
This guide aims at helping them understand and integrate the provisions of the legislation in their business. "

Beatrice Klose
INTERGRAF Secretary General

What is the European Data Protection Regulation?

The European Data Protection Regulation adopted in April 2016 is designed to enable individuals to better control the use of their personal data.

The legislation is technology-neutral; it applies to online data as well as offline data (e.g. paper filing systems). It applies to the handling of personal data in business-to-consumer as well as business-to-business relations.

Key facts

- The General Data Protection Regulation **(EU)2016/679**, commonly known as the GDPR, replaces Directive 95/46/EC.
- Contrary to the former Directive which was transposed into national legislation, the GDPR is a **Regulation** and is therefore directly applicable.
- The GDPR is applicable to all EU Member States as well as **EEA** (European Economic Area) countries.
- Companies and organisations will have to be compliant with the Regulation by **25 May 2018**.

What is the origin of the European Data Protection Regulation?

Data protection has up to now mainly been regulated in the European Union under a 1995 Directive that controls the processing of personal data, which European Member States had to implement into their own national legislation. The world of data today is significantly different from how it was in 1995. In order to catch up with the advances of the digital age, an important adaptation of the legal framework was needed.

The initial discussions on the review of the 1995 Directive started in 2011. At that time, the European Commission wanted to change the way people receive direct mail by changing it from an 'opt-out' to an 'opt-in' situation where people would have to voluntary add their name to a list to receive direct mail. This could have had catastrophic effects for the printing industry. Intergraf research found that a provision like this could negatively affect up to 30% of total print production, leading to a loss of more than 15% of the European printing industry's turnover.

Intergraf strongly advocated against this change of approach by demonstrating that processing of postal direct mail has never been questioned for its ability to respect personal data.
Following a successful lobbying, the European Commission proposed a text with no mention of an opt-in approach, which was replaced by the 'right to object' which guarantees the possibility for people who receive direct mail to opt out.

Moreover, the European Commission's proposal did not foresee that personal data could be processed by a third party. Intergraf advocated for the inclusion of third parties in the legal text securing printing companies can process addresses for direct mail purposes on behalf of their customers.

How are European printers impacted?

The Regulation impacts any company and organisation that is holding personal data, including personal data of its staff. Printing companies are particularly targeted considering their regular use of personal data. The Regulation obviously has an impact on printing companies which activities are related to direct mailing but not only. Printing companies which are using, storing and/or processing personal data provided by customers are also falling under the scope of the Regulation.

In order to best describe printers' liability under the General Data Protection Regulation, this guide provides 3 case examples, which will help all printers identifying their own obligations in respect to their own use of personal data in their regular activity. It ranges from using personal data (company A), to storing (company B) and collecting personal data (company C).

Key definitions

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; and

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1. Use of personal data

Company A

Company A is a user of personal data. It is a **magazine printing company** receiving the subscribers' addresses from its customer, the magazine publisher, by FTP (File Transfer Protocol). Data (name and address) are printed on a label and the magazine is mailed to subscribers by the printer. The printing company does not process further the data but may either keep the data for the next edition of the magazine or delete the data and await the provision of an updated database from the publisher for the next edition of the magazine.

1.1 Roles

In this scenario, the publisher of a magazine has initially collected the names and addresses of its subscribers and transferred them to a printing company, Company A. From a data protection standpoint, the publisher will be considered the controller and Company A the **processor** given that Company A is processing the personal data on behalf of the publisher. Indeed, Company A is using the subscribers' data in order to send the magazine or journal to those subscribers. The purpose of the processing is defined by the publisher, not the printer. As a result, Company A is not using the data for its own purposes but to provide a service to the publisher. Company A is effectively a service provider who is processing the data on behalf of the publisher.

1.2 Obligations

Unlike the current law which only contains obligations for controllers, the GDPR introduces direct obligations on processors. These include:

- ✓ **keeping records of processing activities**;
- ✓ **implementing appropriate technical and organisational security measures**; and
- ✓ **notifying the controller of any data breach**.

1.2.1 Records

A key feature running through the GDPR is the principle of 'accountability'. Organisations must not just be compliant but must *demonstrate* they are being compliant. If Company A has more than 250 employees (or is printing sensitive data such as medical records instead of addresses), it would need to keep a record of the publisher's name and contact details, the category of processing (ie printing address labels), whether any of the data are being transferred outside the EEA (European Economic Area) and a general description of its security measures. These records need to be available for any Data Protection Authority (DPA, i.e. the national or regional data protection regulator) that may request it.

Sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

In practice, it remains to be seen how often DPAs will actually request processor records. But regardless, processors must maintain records in case they are asked.

1.2.2 Security

Company A as a processor must have **security measures** in place that are *appropriate* to the type of data and the risk involved. Printing medical records, for example, would require greater security than address labels. Moreover, the following factors should be taken into consideration when determining the appropriate security measures: state of current technology; cost of implementation; staff knowledge levels; number of staff with access to data. Measures must cover both the **technical** (e.g., encryption, locked doors, passwords, CCTV) and **organisational** (e.g., appointing a Data Protection Officer or arranging staff training).

> The GDPR provides a non-comprehensive list of **security measures** that may need to be implemented:
> (a) the pseudonymisation and encryption of personal data;
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.2.3 Breach notification

If Company A suffers a data breach it must inform the publisher of this as soon as possible after it has become aware of it. 'Breach' is a wide concept and includes, for example, the database being hacked, a pile of printed address labels being stolen or any personal data being sent to the wrong address.

1.3 Liability

The controller is ultimately liable for the processing activity in question in case of a violation of the GDPR, and is responsible for responding to any requests made by the data subjects (e.g. to access their data) or the data protection authorities.

Nonetheless, from a compliance perspective, controller and processor have similar obligations because they are both bound by a duty to comply with the accountability provisions under the GDPR. One of these requirements is the obligation for the controller and the processor to enter into a **data processing agreement**, which sets out the terms of the data processing.

The data processing terms are usually integrated within the broader services agreement between the publisher and the printer, which sets out for example the number of labels, price, delivery date etc. The GDPR is more prescriptive in that it requires to have a written processing agreement, including in electronic form, in place between a controller and processor that stipulates:

- ✓ **the processor is only processing on documented instructions from the controller;**
- ✓ **employees actually doing the processing have committed to confidentiality;**
- ✓ **the processor has taken the appropriate technical and organisational security measures;**
- ✓ **the processor will assist the controller in fulfilling certain obligations; and**
- ✓ **whether the processor deletes or returns (at the controller's choice) all the data at the end of processing**.

Under the current law, the controller remains liable for any infringements of the processor. However, under the GDPR processors also have a general obligation to comply with the

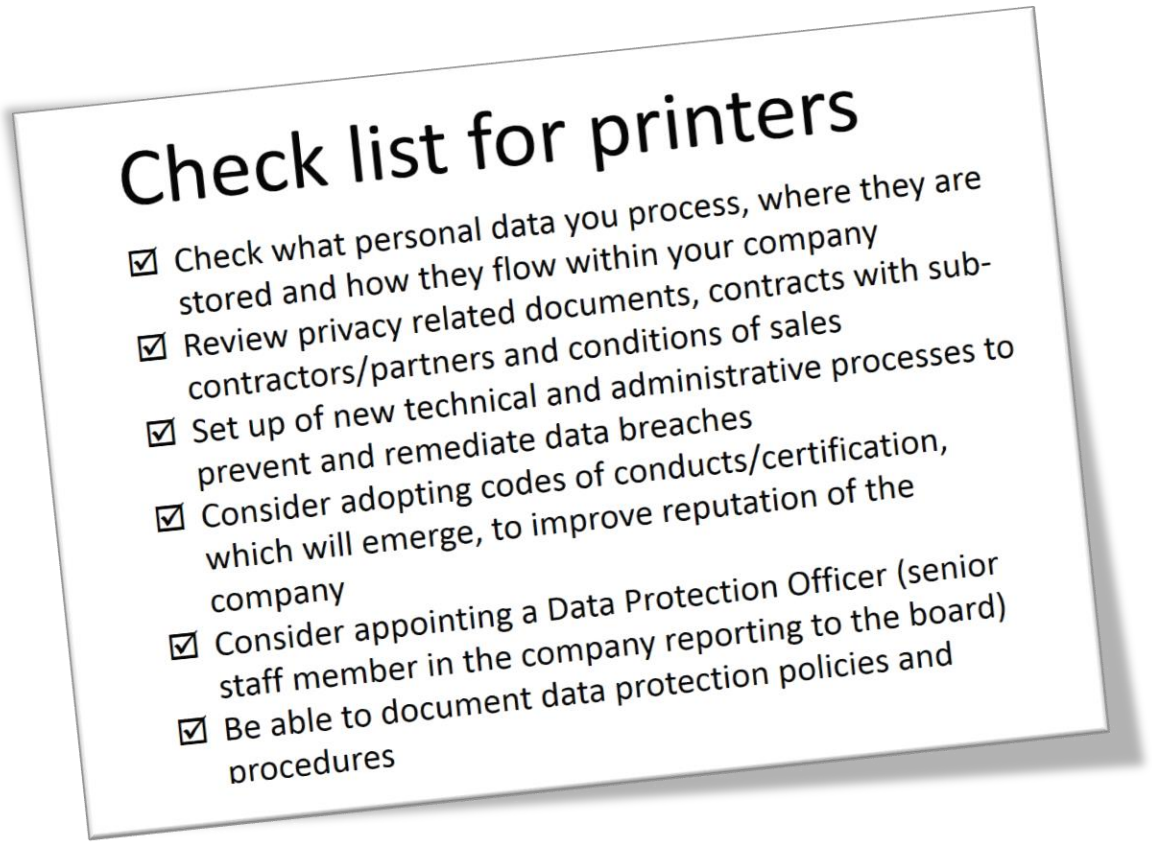
GDPR from a compliance perspective and, as a result, may be sued by individuals or be subject to enforcement actions from DPAs. Enforcement could mean a warning, an audit or fines of up to 4% of annual global turnover or €20m (whichever is the greatest).

As such, processing agreements between publishers and printers will have to be more carefully drawn up to set out liability. One will need clear clauses stating which party is liable in the event of a data breach, for example. It will be a question of fact in each case as to who was to blame.

1.4 Data use

Company A may only process the data on the publisher's instructions, which involves printing the address labels.

By deleting the data and awaiting an updated database, Company A is complying with the data protection principles of accuracy and storage limitation. Keeping the data for the next edition of the magazine is also compliant, assuming magazines are published regularly. Company A should delete the address list if the magazine closes.



2. Storage of personal data

Company B

Company B is a direct mail printing company offering **database management services** to its customers. The printing company has a web platform that gathers data from its customers. The printing company ensures the maintenance of the database (update addresses) but would not do any prospection of clients or profiling. It may sub-contract the job to a company specialised in database management but would remain liable towards its customer.

2.1 Roles

As in scenario A, Company B is considered a **processor** here, processing data on behalf of its customer, the controller. Processing includes **collecting**, **storing** and **amending** data.

If Company B subcontracts the maintenance to a database management specialist, it would remain the processor and the specialist company would be its **sub-processor**. Before subcontracting, Company B should ensure that it has initially received a written authorisation of its customer, the controller.

2.2 Obligations

The obligations of Company B are the same as for Company A detailed at 1.2 above. If Company B were doing the database maintenance itself, it may need increased security as this is a more risky form of processing than Company A's.

If Company B subcontracts the maintenance to the specialist company, under the GDPR it would need to have a written agreement in place which flows down the same obligations as between the customer and Company B. The agreement would need to include all the stipulations listed at 1.3 above. This would apply to any other subcontractors Company B used to process this data.

2.3 Liability

As in the above scenario, both Company B and its customer would be liable under the GDPR. It would depend on who was at fault for any particular infringement and what the processing agreement provides.

If Company B subcontracts the maintenance, it remains fully liable to its customer for any data protection failings of the specialist company. This is very important, given the significant new fining powers under the GDPR. Printers should undertake **due diligence on any subcontractors** where high risk processing is involved.

2.4 Data use

Company B may maintain the database as that is a lawful use and was the purpose for which the data were collected. However, Company B would not be able to undertake any prospection of clients or profiling as those are incompatible purposes.

All processing must have a legal basis to be lawful. The two relevant bases are the individuals' consent or the controller's legitimate interests (explained further under section 3.4 below). Company B's customer may have asked all its clients whether they object to Company B maintaining their details. Under the GDPR, the customer would be prevented from changing the purpose to profiling unless it sought new consent from its clients before doing so.

More likely, the customer assessed it was within its legitimate interests and not contrary to the rights of its clients to maintain an accurate list. If so, the customer would be able to make an assessment as to whether the new process of prospecting clients or profiling would be compatible. In doing so, it would need to consider any link between the initial and further purpose, the relationship between itself and its clients, the nature of the data, the consequences of the further processing and the existence of any safeguards.

Either way, it would be for the customer, as controller, to make that decision. Company B can only process data on its instructions and cannot decide to process for a new purpose. Were Company B to start making those kinds of choices it would be in breach of the processing agreement and would assume the controller role. Therefore, the organisation that determines the means and purposes of processing (i.e. the publisher) is the controller.

3. Collection of personal data

Company C

Company C is a **direct mail printing company offering direct marketing services** (including, prospection of new customers, identifying consumers' preference, profiling activities) to its customers. It may sub-contract the job to a company specialised in direct marketing but would remain liable towards its

3.1 Roles

In this scenario, the role of the direct mail printer as a controller or processor will depend on whether it is carrying out the marketing campaigns on its own behalf or on behalf of its customers.

If Company C is acting on behalf of its customers who are outsourcing the direct marketing operations to Company C, in that case Company C would be considered a **processor** and its customer would be the controller. If Company C subcontracts part or all the processing (e.g., the profiling) to a direct marketing specialist, it would remain the processor and the specialist company would be its sub-processor.

However, if Company C were to use the data for its own marketing purposes, this would make it a controller acting on its own initiative, and it would become directly liable towards the data subjects (which would include an obligation to provide notice and obtain prior opt-in consent from the individuals concerned).

3.2 Obligations

The obligations of Company C are the same as for Company A detailed at 1.1 above. As in scenario B, should Company C subcontract the profiling, it will need an agreement with the specialist company containing the same stipulations as in 1.3 above.

3.3 Liability

As in the above scenarios, both Company C and its customer would be liable under the GDPR, depending on the facts. Should Company C subcontract the profiling, it would remain fully liable for the actions of the speciality company.

3.4 Data use

If Company C conducts the profiling itself, it may need to first assess whether it is compliant. Under the GDPR, impact assessments are required where processing is 'high risk', which includes profiling that has legal effects on individuals. Postal mailing lists are unlikely to fall within this category but further guidance on what constitutes 'high risk' is expected later this year.

Again, it would be the controller who decides the legal basis of the processing. As above, this will generally be the customer unless Company C determines the purposes and means of processing. The two relevant bases are:

(a) Consent

Under the GDPR, consent must be 'unambiguous', separated from consent to all other services and written in plain language. Individuals must be informed about the uses made of their personal data in a privacy notice at the time of collection of their data and must be given the possibility to withdraw their consent at any time. Consent must involve an 'affirmative act signifying agreement' and marketers will need to keep a record of consents, which may involve putting a new system in place.

In the case of direct marketing by electronic means, marketers must obtain prior opt-in consent (or in some cases a "soft" opt-in may apply) in accordance with the e-Privacy Directive. Prior consent would typically not be required for postal marketing. Marketers should therefore check whether the consents they hold from the data subjects are still valid under the GDPR. Most European countries have a suppression list for individuals who have objected to receiving direct marketing mail and so marketers should check their mailing lists against those suppression lists regularly to ensure compliance.

(b) Legitimate interest

The GDPR expressly states that processing for direct marketing may be considered a legitimate interest. DPAs, however, clearly favour consent as a legal basis for direct marketing, particularly as it is required for any form of electronic marketing.

Legitimate interests must be lawful, clearly articulated and represent a real interest. The controller must balance its own interests with the rights of the individuals. In doing so it should take into account the nature of the data, the manner of processing, the reasonable expectations of the individuals and its status in relation to the individuals. Profiling will increase the efficiency customer's marketing efforts whilst providing individuals with more relevant material, which is likely to satisfy the legitimate interest test. Were Company C to combine the data with other data sets then sell the combined profiles to an unrelated party for profit, it would likely fail the legitimate interest test.

Rules on profiling are stricter under the GDPR: individuals will retain the right to object to direct marketing, but this will be extended to profiling and involve obtaining human intervention and an intelligible explanation of the logic involved.

Check the information available from your national data protection authorities!

Some have for example published practical guides for companies:

A practical guide to IT security, ideal for the small business (UK)
https://ico.org.uk/media/1575/it_security_practical_guide.pdf

Règlement général sur la protection des données, préparez-vous en 13 étapes (BE)
https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

Algemene Verordening Gegevensbescherming, bereid je voor in 13 stappen (BE)
https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf

Il nuovo regolamento europeo in ambito privacy: Quali sono i punti di attenzione per le aziende italiane? (IT)
https://users.dimi.uniud.it/~antonio.piva/files/Inf_aziende_2015/Privacy/H%20-%20Nuovo%20Regolamento%20e%20aziende%20italiane.pdf

Guida al nuovo: Regolamento Europeo in materia di protezione dei dati personali (IT)
http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati

La dovela central del Reglamento Europeo de Protección de Datos (RGPDUE) (ES)
http://www.aspectosprofesionales.info/2016/09/la-dovela-central-del-reglamento.html

CONTACT US:

INTERGRAF
Avenue Louise 130A
B-1050 Brussels

Tel: +32 2 230 86 46
Fax: +32 2 231 14 64
Website: www.intergraf.eu