IBA/IFA 34th

ANNUAL JOINT CONFERENCE

*** * * * ***

A NEW ERA IN INTERNATIONAL FRANCHISING

*** * * * ***

NEWS FROM AROUND THE WORLD

THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR):

TIME FOR A CHANGE OF PERSPECTIVE

–

May 9, 2018

Washington, D.C. U.S.A.

Dagmar Waldzus

Buse Heberer Fromm PartG

Hamburg

Germany

The European General Data Protection Regulation (GDPR):

Time For A Change Of Perspective

1. Background

A common level of data protection has been in force throughout the EU and within the European Economic Area since 1995, following the entry into force in October 1995 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[1]

However, the Directive has been interpreted differently in different Member States of the EU. And as a Directive, its provisions were not directly applicable, but required implementation by each Member State. At the beginning of 2012, the EU Commission therefore presented a concept to reform the data protection in the EU. 3100 amendments and almost two years later, on 21.10.2013, the European Parliament adopted its negotiating position which was then confirmed by the plenary on 12.03.2014. After further negotiations until mid-December 2015, the GDPR as finally adopted on 27.04.2016 was published and entered into force on 24.05.2016.[2] The transitional period of two years (some call it "grace period") ends on 24.05.2018, and from one day later on its 99 Articles will replace the provisions of the Data Protection Directive and shall be binding and directly applicable in all Member States.

For EU legislators, this marks the end of an exhausting and long process in which the greatest challenge was to reconcile the diverse interests of the industries on the one hand and individual citizens and data protection advocates on the other, as well as to harmonize divergent views between Member States.

Individuals as data subjects can look forward to a greater degree of transparency as to what actually happens with their personal data when visiting a website, ordering online, joining loyalty programs, and others, and they will be entitled to a faster reaction in case they suspect that their personal data have been used inappropriately.

For the actual addressees of the GDPR, i.e. individuals, companies, and organizations processing personal data, on the other hand, the phase of a raising awareness and taking necessary steps towards compliance seem to be only beginning. It is quite amazing that - according to surveys carried out only a few months before the GDPR will become binding law - the majority of questioned enterprises had not yet taken any or only a few steps towards its implementation within their organization.[3] In December 2017, only about five per cent of the surveyed businesses in Germany had already implemented all the measures required by the GDPR.[4] In view of the high degree of necessary administrative organisation and the risk of severe fines in the absence of compliance, it is certainly not exaggerated to say many businesses in Europe - at least shortly before the due date - have opted for repression rather than for activism.

---

[1] Official Journal of the European Union, L 281, 23.11.1995 p. 0031 - 0050)

[2] Official Journal of the European Union, 04.05.2016, L 119

[3] Senzing Report of January 2018 https://senzing.com/wp-content/uploads/2018/02/Senzing-GDPR-Report.pdf: "Lack of readiness is rampant; Underestimated time to find data; concerning knowledge gap; SMEs are especially at risk.").

[4] ZEW Industry Report of December 2017 http://www.zew.de/en/presse/pressearchiv/eu-datenschutz-grundverordnung-unternehmen-in-deutschland-stehen-unter-anpassungsdruck/

By doing so, (franchise) businesses may miss a unique chance of building trust with customers, understanding data protection as an advantage in competition, and gaining an additional marketing instrument.

2. What's new?

The GDPR aims at further harmonizing the level of data protection within the EU and giving it a higher priority. Nevertheless, not everything is new. The following three major changes (of all others) are worth to be mentioned in advance:

2.1. Reversal of the burden of proof

The burden of proof has been reversed. Before the GDPR came into effect, the data subject had to demonstrate that his or her data had not been processed appropriately. With the effective date of the GDPR, it is the controller processing personal data that must prove that it has acted properly in the event that a data subject (e.g. a former employee, a franchisee, a customer, or a supplier) alleges that his or her personal data have not been processed in compliance with the GDPR.

This fact alone has far-reaching consequences for the future organization of data protection within business organizations and within franchise networks in particular. The essential task now is to be able to demonstrate compliance in a fast and comprehensible way to data subjects and to data protection authorities. And this documentation obligation is associated with considerable organizational effort.

2.2. Market place principle

The circle of affected individuals has also increased considerably in comparison to the situation under Data Protection Directive 95/46/EC, due to the additionally applicable market place principle: if personal data are processed in connection with offers of goods or services in the EU, or, if by processing of personal data the behaviour of individuals in the EU shall be monitored, the processor must comply with the requirements of the GDPR, regardless of whether the processor is located in or outside the EU.

2.3. Increased level of fines

The fines in the event of non-compliance have been massively increased: violations of the general principles applicable to the processing of personal data as described below may result in a fine of up to EUR 20 million or up to 4% of a company’s total global annual turnover of the previous financial year as well as measures by the supervisory authority (Art. 83 (5) a) GDPR).

3. Subject-Matter and Objectives of the GDPR

3.1. General principles

When evaluating which steps are to be taken into which direction in order to comply with the GDPR requirements, franchise networks should keep in mind what the objectives of the GDPR

actually are. By doing so, the potentials and positive effects may outweigh the risks and the costs involved.

The objectives of the GDPR are the protection of the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data (Art. 1 (2) GDPR) and the free movement of personal data (Art. 1 (3) GDPR).

This is nothing really new. But customers realize more and more clearly that their personal data represent a precious asset to marketing departments, and that this does not necessarily come along with appreciation. Appreciation from a customer's perspective requires in a first instance to demonstrate respect for the data subject's decision to actually share personal data. The term "valued customer" must be filled with life and the GDPR offers help.

When processing personal data, the following general principles must be adhered to in accordance with Art. 5 (1) GDPR:

- Lawfulness
- Fairness
- Transparency
- Use for defined purpose only
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

3.2. The right to be forgotten

Another new aspect of the GDPR concerns a person's "right to be forgotten", which is now codified throughout Europe. The right of correction, blocking and erasure already regulated in some EU countries has thus been supplemented and the core element of an ECJ ruling of May 2014 has found its way into codified law.[5]

4. Who is affected by the GDPR and where does it apply?

In short, anyone, i.e. individuals, companies, and organizations alike, who process personal data automatically or store them in a non-automated way must adhere to the GDPR. The GDPR therefore affects micro-enterprises in the same way as global companies, and companies whose business model is based and dependent on the use of personal data as well as small businesses with paper files and customer cards made of carton.

4.1 Material Scope

The starting point for determining the material scope of application is Art. 2 (1) GDPR:

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

[5] Decision C-131/12, 13.05.2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

In this context, a closer look at the definitions in Art. 4 GDPR helps to understand the essential terms:

(i) Personal data

If no personal data are concerned, the GDPR is not applicable. However, the concept of personal data is very broad: it not only includes information such as an individual's name, address, telephone number, a license plate number or IP address. According to Art. 4 (1) GDPR, it is sufficient if a natural person is identifiable directly or indirectly, in particular by assignment to an identification such as a name, an identification number, location data, or one or more special characteristics. Identifiability on a theoretical level is sufficient, e.g. as a result of the aggregation of data.

(ii) Processing

Art. 4 (2) GDPR defines what "processing" actually means, and it is important to be aware of the fact that non-automated means may still fall under this definition:

‚'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;"

As far as automated processing is concerned, this includes of course the use of devices such as computers and smartphones, but also cameras, webcams, scanners or even copiers are covered. Any use of computers, Internet and e-mail can therefore lead to the applicability of the GDPR if personal data is involved.

Non-automated processing is particularly present in the case of handwritten recordings. The intention to include personal data in a file system is therefore sufficient for the application of the GDPR.

4.2. Territorial Scope

The geographical scope of the GDPR is not limited to the EU. Basically, the GDPR applies to the processing of personal data, insofar as this takes place in the context of the activities of a controller or a processor in the EU, irrespective of whether the processing takes place in the EU (Art. 3 (1) GDPR).

Where the processing of personal data of data subjects who are located in the EU is carried out by a controller or processor who is not established in the EU, the GDPR applies, if

- goods or services are offered to data subjects in the EU, irrespective of payment obligations, or
- the behaviour of the persons concerned shall be monitored as far as their behaviour takes place in the EU.

The GDPR also applies to a controller who is not established in the EU but located at a place governed by the law of a Member State under international law (Article 3 (3) GDPR).

The territorial scope cannot be changed by contract or be excluded by a choice of law clause.

5. New requirements with regard to technical and organizational measures

Art. 25 GDPR extends the requirements for technical and organizational measures. This provision is addressed not only to controllers, but also to developers of IT systems and products.

5.1. Data protection by design

Data protection by design (data protection through technology) means that data protection and data security should already be taken into account in the planning and development of IT systems. Thus, data protection and data security requirements should not only be implemented after the instalment of IT systems by expensive and time-consuming additional programming, but instead, possibilities such as deactivation of functionalities, anonymization or pseudonymization as well as authentication, authentification or encryption should already be considered during the development process and the installation.

5.2. Data protection by default

Not everybody is an IT expert, and this is acknowledged in Art. 25 GDPR. Data protection by default (data protection-friendly settings) means that IT systems should be pre-set to be data protection-friendly. The settings are to be defined in a way that only those personal data are processed which are necessary for the purpose pursued in each case. The rationale behind this principle being that many users do not have sufficient IT knowledge and therefore cannot make any settings to protect their personal data on their own. Furthermore, companies must provide the user with functionalities with which he can protect his privacy (e.g. encryption).

6. Cross-border data processing

6.1. International data transfers to third countries

The transfer of personal data to countries outside the EU or the EEA to so-called third countries remains problematic. This was already the case under Directive 95/46/EC and will remain so with the GDPR, the reason for this being to ensure that the level of protection of individuals granted under the GDPR is not undermined. The general assumption here is that there is no adequate level of data protection in third countries, unless the EU Commission has established one for the country concerned. Accordingly, data transfers to third countries will only be permitted in the future if additional security mechanisms help to ensure an adequate level of data protection or if such an adequate level has been established as binding.

(i) General principles

In principle, the rules laid down in Directive 95/46/EC continue to apply. Therefore, if there is a legal basis for the general transfer of data, the instruments already available before the GDPR became applicable can continue to be used to transfer data to a third country. Mechanisms for establishing an adequate level of data protection include, for example:

- Binding Corporate Rules (BCR): binding, self-imposed company regulations on the handling of personal data
- EU standard clauses: model clauses developed by the EU Commission, the content of which may not be modified.

In addition, the other data transfer options as provided for in the Data Protection Directive also remain applicable. According to Art. 49 GDPR for example, it is possible to transmit personal data on the basis of consent or in order to fulfil a contract. Decisions of the Commission relating to an adequate level of data protection in a given country, which have been taken on the basis of the Data Protection Directive, also remain in force until they are amended, replaced or repealed by a decision by the Commission under a review procedure as laid down in the GDPR.

What is new is that the GDPR allows to establish an adequate level of data protection for one or more specific sectors of a third country. Therefore, data transfer without further transmission-specific measures is also permitted to processors within such areas or sectors.

Binding Corporate Rules are now specifically regulated in Art. 47 GDPR, which lays down, among other things, minimum requirements with regard to the necessary content.

(i) Data transfer to the US: the EU-US Privacy Shield

If companies in the EU use cloud computing solutions from providers based in the US or whose servers are located in the US, e.g. for e-mail marketing, or if franchisees in the EU are required to transfer personal data to their franchisor in the US, the EU-US Privacy Shield as effective since 12 July 2016 is still the legal basis for such data transfers after the ECJ's decision of 6 October 2015 resulting in the overturn of the Safe Harbor Agreement. When transferring personal data for processing in the US the following must be observed:

- Does the processor in the US have a valid certificate? (To be checked under www.privacyshield.gov/list)
- Where processing is to be carried out on behalf of a controller, are the requirements of Art. 28 and 29 GDPR fulfilled?

As things stand at present, the Privacy Shield will continue to apply after the GDPR has become binding but is continuously subject to critical scrutiny by data protection activists in the EU in particular.

6.2. One Stop Shop

In practice, data protection officers are often confronted with divergent legal opinions of several data protection supervisory authorities concerned. This problem is taken into account in the GDPR, because Article 56 (1) GDPR introduced the principle of the One Stop Shop for cross-border data processing.

Pursuant to Art. 56 (6) GDPR, in the case of cross-border data processing, the so-called lead supervisory authority is the sole point of contact for the controller or the processor. In the future (in an ideal world), companies will only have one contact for assessing data protection issues in cross-border data transfers or processing, on whose statements they can then also rely.

Art. 56 (1) GDPR states that in the case of cross-border data processing, the lead supervisory authority shall be the supervisory authority of the main establishment or of the single establishment of

the controller or processor. Data protection experts are in agreement already on the complexity of the assessment factors for the determination of the lead supervisory authority.

7. Is there any change in the requirements for effective consent?

The essential requirements for effective consent remain unchanged. There are only some amendments with respect to the protection of minors.

7.1. Data protection is protection of fundamental rights

The consent of the data subject to the processing of his or her personal data has always been a central element of data protection law in the EU and its Member States: each individual has a right to data protection, privacy and informational self-determination. These rights are guaranteed not only in national laws or constitutions of the Member States, but also by the EU Charter of Fundamental Rights, which expressly protects the personal data of individuals in its Article 8.[6] With the consent, the person concerned is enabled to dispose of his or her personal rights and to disclose personal information about himself or herself or not.

7.2 Prohibition with reservation of permission

In data protection law, the general principle of prohibition subject to permission applies: data processing is therefore generally prohibited as long as it is not expressly permitted by law or the data subject has consented to the processing. The GDPR also maintains this principle in Art. 6 (1) a) GDPR.

Art. 7 GDPR describes the "conditions for consent". Before submitting the declaration of consent, the data subject must be informed in detail about the intended purpose of the collection, processing or use of his personal data. He must also be able to easily recognize the information and identify it as consent. The declaration of consent of the data subject must be voluntary, i.e. the individual must be able to make a real choice. In the course of obtaining consent, the individual may not be presented with a fait accompli or otherwise restricted in its decision-making power (see also Art. 7 (4) GDPR: “utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”).

Art. 7 (1) GDPR only requires the controller to be able to demonstrate the consent, whereas a particular form is not stipulated. Recital 32 clarifies that consent should be given by a clear act, which can also be done electronically. Thus an active action of the data subject by Opt-In (e.g. setting a checkmark) is necessary, while e.g. an implicit agreement or Opt-Out (e.g. removing a checkmark) is no longer possible and/or sufficient.

The data subject has a right to revoke the consent, and he or she must be informed about this right of revocation before giving the consent. Revoking the consent must be as easy as giving it (Art. 7 (3) GDPR).

What is new is the provision in Art. 8 (1) GDPR according to which the consent of minors under 16 years (or under 13 years, if the national law so provides) is only effective if and insofar as this consent is given by the holder of parental responsibility on behalf of the child or with the child's consent.

[6] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 18.12.2000, C 364/01

8. Conclusion

The GDPR forces franchisors to actively pursue data protection, an aspect which may have received less attention in the past. After the management and executives have recognized the need for action and have analyzed the current situation in their own organization, have identified the areas where action is required and have decided whether or not to engage an external data protection officer, the corresponding processes in which personal data are processed must be adapted and documented.

8.1 Data protection management in the franchise network

The measures described above (and many more set forth in the GDPR) also present franchisors with the task of making fundamental data protection decisions in conjunction with their franchisees and reviewing past decisions in this respect. Franchise agreements must be reviewed and, if necessary, updated in the light of provisions already adopted on data protection.

In addition, franchisors may use the opportunity to make strategic considerations with regard to their data protection management in general.

Several alternatives are conceivable: the franchisor can decide to keep himself out of the liability for data protection violations of the franchisees as far as possible. The franchisor would then have to ensure that no personal data of the franchisee's employees, customers, or suppliers can be accessed. By taking this approach, the franchisor must be ready to accept only limited response if the franchisee's failure results in compliance violations that cause damage to the reputation and the brand of the entire franchise network.

The franchisor may also decide to impose on its franchisees a network-wide data protection management in order to ensure a uniform and in many cases also higher level of data protection in the entire system. In this case, appropriate contractual agreements with the franchisees must be concluded, which, in view of the detailed requirements of the GDPR, must go beyond the standard clauses often used in franchise agreements prior to the entry into force of the GDPR. The higher degree of control is accompanied by the risk of the application of a higher fine, because then the data protection authorities will take into account for the assessment of the fine the turnover of the entire network. If a network-wide data protection officer is appointed, the associated costs may be passed on to the franchisees subject to a proper arrangement with them.

8.2. Entrusting a third party processor with processing

In many franchise networks, the services of external providers are engaged, e.g. to send mailings and newsletters or to point out new offerings to customers. Further, franchisors often reserve the right to use certain data of their franchisees for benchmarking purposes and in that respect also use external service providers.

Since, according to the GDPR, each data subject must have been informed accordingly before their personal data is processed and their consent or any other legal basis must be documented, an essential task for franchisors will be to analyse whether the requirements of the GDPR in connection with the engagement of service providers are met and to increase their franchisees' awareness of this. In most cases, new arrangements will have to be negotiated.

8.3. Data transfer to third countries

If services from providers are used whose location is outside the EU, or if the franchisor is located outside the EU, i.e. in a third country, it is now imperative to closely monitor the existing data flows to the provider and to the franchisor and to check whether a level of data protection appropriate to the requirements of the GDPR is guaranteed.

For the data transfer from the EU to the US, the Privacy Shield continues to apply. However, in view of the repeated criticism of this Agreement and in view of the fact that the EU standard contractual clauses are currently under review by the ECJ following a submission by the Irish High Court, franchisors may be well advised to consider alternatives. Should the Privacy Shield suffer the same fate as Safe Harbor, franchise networks could be requested by the competent data protection authorities at short notice to immediately transfer all affected data to a server within the EU. Whenever the use of cloud services by service providers with servers in the US is not absolutely necessary or preferable for some reasons, franchisors may consider using providers whose servers are located in the EU right away.

Dagmar Waldzus

Dagmar Waldzus is a partner in the Hamburg office of Buse Heberer Fromm, a full-service law firm with 6 offices in Germany. She studied law at the universities of Passau and Hamburg and earned a Master's degree in International Legal Studies from New York University in 1996. Ms Waldzus is the head of the firm's Distribution and Commercial Law Practice Group, and her work is focused on franchise, sales and distribution law. She frequently advises franchisors in relation to the internationalization of their concepts - inbound and outbound. She is an associated expert with the German Franchise Association (DFV), a member of the DFV's Think Tank on Digitalization, a member of IBA's Committee on International Franchising, and a frequent author and speaker on various topics in franchise and distribution law. Ms Waldzus is listed in the International Who's Who of Franchise Lawyers, and has presented programs for the DFV, the German Franchise Institute, the International Bar Association, and the International Franchise Association.