A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

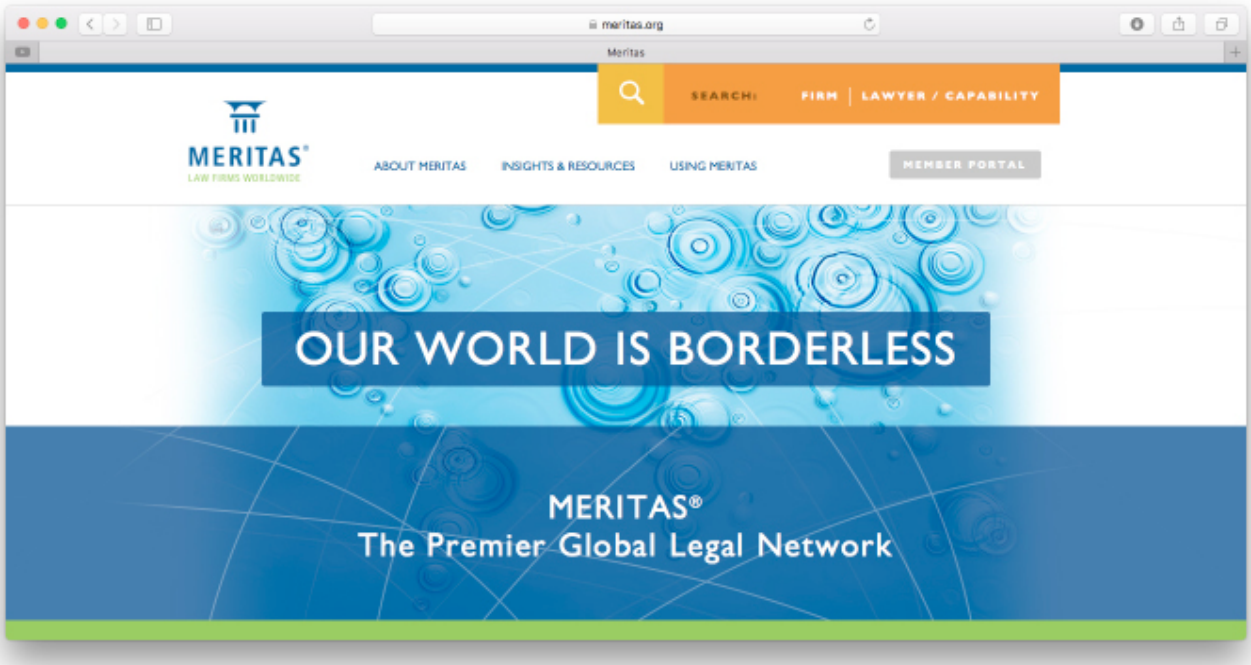
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

GERMANY, EUROPE

FIRM PROFILE:

ARNECKE SIBETH DABELSTEIN

ARNECKE SIBETH DABELSTEIN - The commercial law firm. 12 areas of expertise - focused, reliable, premium! As a leading commercial law firm, we are internationally recognized for our core competencies in real estate, maritime industry, and the transportation/aviation/logistics market.

ARNECKE SIBETH DABELSTEIN provides comprehensively focused legal advice building on a foundation of a total of 12 outstanding areas of expertise. Our expertise is on par with specialized competitors and will continue to grow in the future. We plan to strategically develop the fields of insurance, energy, and sports/media/entertainment to become further core competencies.

ARNECKE SIBETH DABELSTEIN is innovative, dynamic and modern. Proven valuable and successful for decades, as authentic advisors at the highest level we have a proven record of success and value.

Our international network is multi-layered and tightly-knit. As a member of Meritas we are a reliable partner for our international clients.

CONTACT:

HANS GEORG HELWIG
h.helwig@asd-law.com

+49 30 8145913-42
www.asd-law.com

MERITAS®
LAW FIRMS WORLDWIDE

FRANCE, EUROPE

FIRM PROFILE:

BignonLebray

Founded in 1982, Bignon Lebray specializes in all areas of company law.

Our firm brings together more than one hundred legal professionals, including 25 partners, specialising in 11 practice areas.

Our cultural and professional diversity reflects our history: we are an independent French law firm that has evolved with its clients as they seek growth in today's globalized business world.

We provide services to companies ranging from small start-ups to large listed firms and to public authorities and not-for-profit organizations. Central to our legal focus in all matters, legal and contentious, is a thorough understanding of our clients' business activities and projects.

Through our 4 offices in France (Paris, Lyon, Lille and Aix-Marseille), we endeavor to bring clients the most efficient, cost effective and case-specific answers to their business needs.

CONTACT:

ÉLISE DUFOUR
edufour@bignonlebray.com

+33 (0)1 44 17 17 44
www.bignonlebray.com

Introduction

On May 25, 2018, the European General Data Protection Regulation (GDPR) came into force. As legislation directly binding all EU member states, the GDPR is a true paradigm shift. In the past, while statutory provisions did protect data subjects' rights, a violation was not a barrier because fines for international enterprises were small. Now, any infringement could cost businesses up to 4% of their worldwide revenue or up to 20m EUR. Protection of personal data must now be taken seriously. Below is a general outline based on 11 questions we are asked regularly about the new regulation. Also rendered are references to how German and French law will apply the GDPR in the respective countries. As an EU regulation the GDPR is directly applicable and takes direct effect in each EU member state, superseding contradictory national laws. Yet, in some aspects the GDPR allows for the member states to implement individual national provisions that are stricter than the GDPR.

1. What are the major personal information protection laws or regulations in your jurisdiction?

The REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. Its key points of impact are:

(1) Extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location;

(2) Severe penalties (see above).

(3) Stricter conditions for valid consent given by a data subject.

(4) Right to be forgotten, data portability.

(5) Mandatory data protection officers to be appointed by enterprises.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Although directly applicable, this regulation has been incorporated into domestic law on June 20th, 2018.

The Federal Data Protection Act 2018 (abbr. BDSG), implements the GDPR.

Where permissible by the GDPR the BDSG stipulates even stricter rules.

2. How is personal information defined?

Art. 4 (1) : (1) "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Information about corporations or companies is not included in the definition, which is limited to the personal information of individuals, but information identifying members of a corporation can be.

Personal data of deceased persons is not protected under the GDPR (Recital 27). Member states may, however, stipulate rules with respect to such data and its continuous protection after a person's death.

According to Art. 2 of the law, the same definition as in GDPR applies.

BDSG refers to Art. 4 GDPR and therefore does not stipulate a more detailed definition. According to German case law, however, the business email address of an individual is considered 'personal data'.

3. What are the key principles relating to personal information protection?

Chapter III GDPR: Data concerning individuals can be collected, provided that they have been informed of this operation. (Art. 13)

Art. 5: personal data shall be:

(1) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…);

(3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(4) Accurate and, where necessary, kept up to date (…) ('accuracy');

(5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (…) ('storage limitation');

(6) Processed in a manner that ensures appropriate security of the personal data ('integrity').

Recital 39 with respect to the storage time stipulates: What requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

According to article Art. 6 of the law, the same rights are stipulated.

BDSG refers to the GDPR and therefore stipulates the same rights.

4. What are the compliance requirements for the collection of personal information?

Art. 6 GDPR: Processing shall be lawful only if and to the extent that at least one of the following applies:

(1) The data subject has given consent to the processing of his or her personal data for one or more specific purposes [according to Art. 7 and recital 32 – consent does not have to be given in writing; whereby the controller should demand consent in writing to be able to prove that consent has been given, Art. 7 Sec. 1 GDPR];

(2) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(3) Processing is necessary for compliance with a legal obligation to which the controller is subject;

(4) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(5) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Art. 13 GDPR: the data subject should be informed at the time of:

(1) The identity of the data controller;

(2) The purpose;

(3) The compulsory or optional nature of the answers;

(4) Possible consequences for him of a failure to reply;

(5) Recipients or categories of recipients of the data;

(6) The rights the data subject has according to the law;

(7) Where appropriate, transfers of personal data to a non-member State of the European Community;

(8) The retention period of the categories of data processed.

According to Art. 32 of the law, the same requirements are provided.

Sec. 32 to 37 of Germany's Federal Data Protection Act establishes the same regime.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

See answer to Q4.

The disclosure of personal data shall only be admissible with the consent of the data subject.

According to Art. 34 of the law, the data controller should take all appropriate precautions, in view of the nature of the data and the risks presented by the processing, to preserve the security of the data and, in particular, to prevent them from being distorted, damaged, or that unauthorized third parties have access.

See answer to Q4.

If personal data are obtained not from the data subject but a third party, Art. 14 GDPR and Sec. 33 BDSG stipulate specific rights of information vis-à-vis the controller, such as:

(1) Identity and contact details of the controller and data protection officer;

(2) Purpose for processing of personal data and legal basis;

(3) Categories of data concerned;

(4) Recipients of data;

(5) Ensure fair and transparent processing, which includes,

- Period of storage
- Rights according to Art. 5 GDPR
- Right to lodge a complaint with a supervisory authority
- Source personal data originates from

(6) Such information must be provided within a reasonable time after obtaining the data.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

Art. 44 to 50 GDPR.

The transfer is not possible, provided safeguards are taken such as:

(1) Standard EU agreement (Data Controller to Data Controller and Data Controller to Data Processor);

(2) Binding corporate rules;

(3) Transfers or disclosures to a country with an adequate level of protection.

If the controller fails to take such measures of an adequate level of data security, it shall be personally liable towards the data subject according to Art. 82 GDPR. In addition, an infringement of Art. 44 to 49 GDPR is subject to administrative fines up to 20m EUR or up to 4% of the yearly turnover according to Art. 83 Sec. 5 GDPR.

According to Art. 69 to 70 of the law, the data controller may not transfer personal data to a State that is not a Member of the European Union if this State does not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights.

Some exceptions exist.

The BDSG provides for a very elaborate regime of prerequisites for the transfer of data to third countries in Sec. 78 to 81. This includes:

(1) The transfer of personal data to a third country law enforcement authority if the data subject's fundamental rights are not deemed to be more protectable;

(2) The transfer on the basis of a adequacy decision of the EU commission, based on Art. 36 (3) of the Directive (EU) 2017/680, i.e. the Commission has resolved that the third country in question meets EU data protection standards (the EU commission upholds a regularly updated list on its respective resolutions and states recognized as "adequate").

(3) Without such resolution the transfer to a third country is admissible, if this country has given a legally binding guarantee to give sufficient protection to an individual's personal data, e.g. the US-EU Privacy Shield.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

Art. 12 to 23: GDPR.

(1) Transparent information, communication and modalities for the exercise of the rights of the data subject.

(2) Disclosure of and access to personal data.

(3) Information to be provided where personal data are collected from the data subject, and where personal data have not been obtained from the data subject.

(4) Right to restriction of processing, data portability, of access by the data subject, to rectification, to erasure (right to be forgotten).

(5) Notification obligation regarding rectification or erasure of personal data or restriction of processing data portability.

(6) Right to object and automated individual decision-making.

According to Art. 7 Sec. 3 GDPR the data subject shall have the right to withdraw consent at any time; whereby lawfulness of processing based on the consent before its withdrawal is not affected. Withdrawal further only affects lawfulness of data processing based on consent according to Art. 6 (1) (a) GDPR.

According to Art. 38, 39 and 40 of the law, same rights, but France have an additional right: according to article 40-1 of the law, the data subject also has the right to define guidelines on the fate of his personal data after his death.

Rights of the data subject are stipulated in Sec. 32 et seq. BDSG and resemble the standards of the GDPR.

Besides the general principles laid out in Art. 5 and 6 GDPR (see Q3 and 4) a fundamental change is the establishment of the data subject's right of information according to Art. 13 GDPR, such as (e.g.),

(1) Identity and the contact details of the controller;

(2) Contact details of the data protection officer;

(3) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(4) Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(5) Recipients or categories of recipients of the personal data;

(6) Basis for transfer to a third country;

(7) Period of storage;

(8) Existence of right to object and right of erasure;

(9) Right to withdraw consent at any time, when processing is based on consent (Art. 6 (1) (a) GDPR;

(10) Right to file a complaint to the supervisory authority.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context (Art. 88 GDPR).

The law does not define a specific frame for employees' personal information protection. However, according to the CNIL's decisions, the consent of an employee should be collected with additional safeguards. Indeed, the CNIL considers that the consent of the employee is not freely given and hence not a valid legal ground for processing the data of an employee. Hence the employer should collect data only with regard of the execution of the employment contract or its legitimate interest.

Sec. 26 BDSG implements the provision in the GDPR.

In addition to codified law, within an employment relationship a basis for data processing may also be provided for in collective bargaining and shop agreements.

For example, collective agreements often define rules for the use of IT, especially Internet and email devices. This includes the accessibility of employee's accounts. Without an employee's consent, the employer shall not access the employee's email account, whereas a shop or collective bargaining agreement may stipulate such a right for the employer, which then supersedes a missing consent.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

Telephone: +32 2 283 19 00

Email: edps@edps.europa.eu

Website: www.edps.europa.eu

The CNIL, "Commission Nationale de l'Informatique et des Libertés", is responsible for implementation and enforcement of personal information protection laws in France. CNIL's details are:

CNIL

3, Place de Fontenoy

75007 Paris, FRANCE

Tel: 01 53 73 22 22

The state data protection commissioner – each of the 16 states in Germany has its own commissioner responsible.

Further the Federal Data Protection Commissioner as the national supervisory authority established a so-called single point of contact (ZASt. - www.bfdi.bund.de/ZASt/EN). In the federal German system, which is unique throughout Europe, and which includes data protection supervisory authorities of the Federal Government and of the 16 Länder (Federal States), the single contact point coordinates the cross-border cooperation with the other Member States of the European Union, the European Data Protection Board (EDPB) and the European Commission. The ZASt is established at the Federal Commissioner for Data Protection and Freedom of Information, but organizationally separated from that authority.

As a single contact point, the ZASt shall enable the supervisory authorities of the other Member States, the EDPB and the European Commission, to communicate

effectively with the German supervisory authorities.

It is not active in the external relationship vis-à-vis citizens, authorities and companies.

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

Art. 83 GDPR administrative provides penalties up to 10 or 20 million euros or 2% to 4% of the global turnover (GDPR) depending on the offence.

Article 45

The CNIL can pronounce administrative penalties up to 10 or 20 million euros or 2% to 4% of the global turnover depending on the offence.

In addition, certain offenses are punishable by criminal law and are punishable by five years of imprisonment and a € 300,000 fine (multiplied by 5 for legal entities) (article 226-16 to 226-24 of the criminal code).

Art. 83 GDPR is directly applicable according to Sec. 41 BDSG. Further Sec. 43 BDSG limits the fine to a maximum of 50.000 EUR for infringements of rights of information of the data subject acc. to Sec. 30 BDSG.

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

European Union data protection affects every business and organization and cannot be ignored. The scope of data protection and implementing regulations is likely to increase in the coming years throughout the European Union..

In addition to the GDPR the ePrivacy Regulation is expected to come into force within the first six months 2019. This more towards e-commerce directed regulation was originally intended to be effective parallel to the GD PR on May 25, 2018.

Certainly, all of Europe can expect an increase in jurisdiction relating to violation of the GDPR as the immense fines will force controllers to take legal action against imposed fines.

A recent law for the protection of personal information has recently been adopted: The law n°2018-493 of June 20, 2018, promulgated June 21, 2018, modified the law Informatique et Libertés of January 6, 1978.

The decree implementing the law has been adopted on August 1 2018.

The GDPR has been implemented with the BDSG. ePrivacy will follow.

Conclusion

The European Union is currently composed of twenty-eight countries. Using France and Germany as examples, this outline illustrates how GDPR compliance and obligations may vary from country to country because of differences in national transition laws of EU members and the EU members' different interpretations of the GDPR provisions.

We recommend that your business strictly comply with all standards set by the GDPR. Your obligations may extend beyond what is contained in this outline. For example, your records of processing activities and obligations to delete incorrect information as well as technical and organizational measures should be established immediately.

A violation or non-compliance with GDPR standards and national requirements will expose your business to significant fines. In addition, it may endanger cross-border relations as your business partners will look to you for verification of compliance with all GDPR provisions.

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680