DATH PLLC | Mukilteo Law Firm

Innovative, Responsive, Experienced. We can help.

The Law Offices of Dubs Ari Tanner Herschlip PLLC
DATH PLLC | MUKILTEO LAW FIRM
627-5th St, Ste. 203
Mukilteo, WA 98275
425-903-3505 Phone
425-298-3918 Fax

OVERVIEW OF THE GDPR

Introduction

The European Union's ('EU') new General Data Protection Regulation ('GDPR') that went into effect on May 25, 2018, regulates personal data processed or retained by any individual, company, or organization, which relates to individuals and entities located in the EU. The GDPR applies to the activities of companies if they process or retain such data, even if the processing of relevant data occurs outside the EU. The key to compliance is that businesses must have full consent and an opt-in from users that cannot be confusing. User consent forms must state precisely what data is being collected, what it will be used for and how long the company will store that data. If a business wishes to use data for purposes outside of the original consent, then the business must seek permission from the user before it can happen.

General Data Protection Regulation (GDPR)
Partial Summary of Regulations

- GDPR regulations apply to any company processing or gathering information from an EU citizen.
- The GDPR defines personal data as "information relating to an identified or identifiable natural person." Personal data includes an individual's IP address, device ID, customer reference number and combinations of information that can lead to the identification of a particular person.
- If there is a possibility of your company may process personal data of EU citizens or receive information from an EU citizen, the internet user must be allowed, upon request, to:
  1. Access to their personal data;
  2. The ability to instruct your company to erase their personal data; and
  3. Have the ability to move their personal data from one processing entity to another.
- If your company collects certain data classified as "special category" data, the individual's consent to collect that data must be explicit.
- Companies who process personal data on a large scale must have a data protection officer ("DPO") overseeing compliance.

Does the GDPR apply to our Company?

The GDPR applies to any company or entity, located outside the EU that: (1) processes or obtains personal data of individuals in the EU, regardless of whether or not their goods or services are offered for a price, and (2) companies or entities located in the EU that processes "personal data" as part of their business activities. The GDPR applies to businesses of all sizes, including B2B.

Companies with fewer than 250 employees are required to hold internal records of processing activities if the processing of data could affect an individual's rights or freedoms, or if it pertains to criminal activity. Also, please remember that definitions of "employee" vary across jurisdictions, such that independent contractors may be treated as employees for purposes of this regulation.

For those with more than 250 employees, more detailed records need to be kept. These records include the name and details of your organization, the name of your assigned data protection officer, the reasons for processing the data, a description of the categories of data being processed, details on the recipients of the data, how long it will be retained, details on transfers outside of the EU, and an overview of the security measures your organization has put in place.

However, it's possible that you will need to comply with the more rigid requirements of companies with 250+ employees if you process the personal data of EU citizens on a regular basis. You are only exempt from doing so if you only process EU residents ***occasionally***.

GDPR explicitly states that small and mid-sized businesses need to provide the same level of detail of processing activities as a large enterprise if "the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data... or personal data relating to criminal convictions and offences referred to in Article 10."

What is Personal Data?

The GDPR defines personal data as "information relating to an identified or identifiable natural person." Personal data includes an individual's IP address, device ID and customer reference number.

Different pieces of information collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymized, but can be used to re-identify a person, remains personal data and falls within the scope of the GDPR law. Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible. The GDPR protects personal data regardless of the technology used for processing that data. Likewise, it also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

How complicated is GDPR compliance?

The GDPR is wide-reaching and its impacts your company's departments and/or relationships with service providers including: legal, regulatory compliance, HR, IT, insurance, security, procurement, marketing and customer relations, as well as PR and communications. Be sure to discuss this development with your team of professionals.

The elements of the GDPR, many of which are beyond the scope of this memo, include:

1. Fines
   (Organizations face fines of up to 2% of their annual revenue or €10 million, whichever is higher, for infringing GDPR's code of practice. For actual breaches of people's personal data, that rises to 4% of turnover or €20 million, whichever is higher.)
2. Privacy Impact Assessments
3. Data Protection Officers
4. Email archiving
5. Data transfer rules
6. Data breach notifications
7. Right to be forgotten
8. Network forensics
9. Consent
10. Wider geographic scope
11. Data portability
12. Privacy by design
13. Network traffic analysis
14. Right to erasure

What individual rights are affected by the GDPR?

1. Personal data access
2. Error correction
3. Right to be forgotten
4. Data usage transparency
5. Control personal data usage
6. Data breach notifications

What company responsibilities are affected by the GDPR?

1. Increased responsibility for data
2. Consent requirements
3. Data protection officer
4. Data and network security
5. Data transfer restrictions
6. Data breach notifications and fines

What happens if individuals contact us about their personal data?

Individuals may contact a company to exercise their rights under the GDPR. These rights include the right of access, the right of rectification, the right of erasure, and the right of portability. Where personal data is processed by electronic means, a company should provide means for requests for personal data to be made electronically. A company must reply to a request without undue delay, not to exceed one (1) month from the date the request was received. Companies may ask the individuals for additional information in order to confirm their identity. A company may reject a request for personal data, but must inform the individual of the reasons for doing so and of their right to file a complaint and to seek a judicial remedy. Although such requests should be carried out free of charge, where requests are manifestly unfounded, excessive, or unduly repetitive, a company may charge a reasonable fee or refuse to act.

Individuals have the right to object to the processing of personal data for specific reasons. Individuals also have a right to object at any time to the processing of their personal data for direct marketing purposes. Direct marketing is understood under the GDPR as any action by a company to communicate advertising or marketing material, aimed at particular individuals. A company must inform individuals in its privacy notice, that it will be using their personal data for direct marketing and that they have a right to object free of charge. If a person objects to processing for direct marketing purposes, a company may no longer process their personal data for such purposes. Likewise, if any data was processed unlawfully, or collected from individuals who were minors, then it must be deleted.

Unless personal data has been completely anonymized, the GDPR gives individuals the right to ask for their data to be deleted and companies do have an obligation to do so, except in the following cases:

- the personal data held is needed to exercise the right of freedom of expression;
- there is a legal obligation to keep that data; and
- for reasons of public interest (for example public health, scientific, statistical or historical research purposes).

In the event that a company receives a request from an individual to delete their data, it is required to take reasonable steps, including implementation of technical measures, to inform other websites that a particular individual has requested the erasure of their personal data.

What type of Personal Data can be collected and processed?

Generally, to minimize the risk of unknowingly disclosing personal data, it is preferable to use anonymous data, and personal data should only be processed when reasonably feasible alternatives do not exist. Before collecting personal data, the user must grant express agreement to submit their personal data and know the reason for processing it and for what specific purpose(s) it will be used. Personal data must be processed in a lawful and transparent manner. To that end, personal data may only be collected if there is a specific purpose for doing so, and that purposes must be clearly indicated to the individual with whom that data originates. Collecting data for undefined purposes is impermissible. Additionally, personal data may be used for purposes other than those for which it was originally collected in very limited circumstances. Companies that work in all fields, aside from scientific research, desiring to use previously collected information for new purposes must first check to ensure that new purpose is compatible with the originally asserted purpose. The following factors are considered when making this determination:

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected;
- the type and nature of the data;
- the possible consequences of the intended further processing;
- the existence of appropriate safeguards (such as encryption or pseudonymization);

If the personal data was collected with the individual's consent, additional processing outside the scope of the originally asserted purpose is not permitted without additional consent for the new purpose from that individual.

Obtaining consent to collect personal data

In most instances, consent is required in order to collect personal data. In order for consent to be valid, the following must be true:

- it must be freely given;
- it must be informed;
- it must be given for a specific purpose;
- all the reasons for the processing must be clearly stated;
- it is explicit and given via a positive act (for example an electronic tick-box that the individual has to explicitly check online or a signature on a form);
- it uses clear and plain language and is clearly visible;
- an individual must have a free choice and must be able to refuse or withdraw consent without being at a disadvantage.

Under the GDPR, "special categories" of personal data require EXPLICIT CONSENT

What types of data falls into the "special category?" Data regarding:

- Race or ethnicity;
- Political opinion;
- Genetic data; and
- Union membership.

What is required before and after data is collected or processed?

At the time of collecting their data, people must be informed clearly about the following:

- The colleting company's name and contact information;
- The reasons for which the personal data will be used;
- The categories of Personal Data implicated;
- The legal justification for the processing of the Personal Data;
- The duration that the Personal Data will be stored;
- Who else may receive the Personal Data;
- Whether their personal data will be located or transferred to a recipient outside the EU;
- That they have a right to a copy of the personal data and other basic rights in the field of data protection;
- That they have a right to lodge a complaint with a Data Protection Authority; and
- That they may withdraw consent at any time.

This information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means where appropriate. It must be provided in a concise, transparent, intelligible and easily accessible way, and in clear and plain language, without

charge. When a company obtains this data from third-parties, they should provide this information to the individual within one (1) month after the information was obtained. Companies are also required to inform the individual of the categories of data and the source from which it was obtained even when the information was obtained from publicly accessible sources.

Additionally, both the accuracy and security of information collected is now regulated. Companies must ensure that the personal data they collect is accurate and up-to-date. If any inaccuracies are present, the company must correct it. Similarly, companies must install appropriate technical and organizational safeguards that ensure the security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Demonstrating Company Compliance and Consequences of Non-Compliance:

The GDPR requires companies processing large amount of "special category" data on a large scale to appoint a data protection officer, to ensure the company is GDPR compliant.

The GDPR encourages companies to create data protection certification procedures so they can clearly demonstrate their compliance if needed, such as obtaining an EU-US Privacy Shield. Information regarding the EU-US Privacy Shield can be found at: https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield.

Under the GDPR companies not in compliance with their rules, can be fined as much as four-percent of their global turnover or 20 million euros ($131 million U.S. dollars), relating primarily to breach of consent requirements (see #4 above).

Retention: How long can the personal data be kept?

Companies should only retain personal data for the shortest duration possible. As such, it should be stored only to effectuate the originally asserted purpose for which it was collected, and no longer. Companies should establish time limits to erase or review the personal data stored. That being said, in some instances, personal data may be kept for a longer period for archiving purposes in the public interest, or for reasons of scientific or historical research, provided that appropriate technical and organizational measures are put in place such as anonymization, and/or encryption.

What about personal data obtained from third-parties?

Before acquiring a contact list or a database with contact details of individuals from another organization, that organization must be able to demonstrate that the data was obtained in compliance with the GDPR and advertising use is permitted. For example, if the organization acquired it based on consent, the consent should've included the possibility to transmit the data to other recipients for their own direct marketing. A company must ensure that the list or database obtained from the third-party is up-to-date and that no advertising is sent to individuals who previously objected to the processing of their personal data for direct marketing purposes. Companies must also inform individuals, that their personal data has been collected and that they will be processing it for the purposes of sending advertisements.

What is Data Processing?

Data processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

Examples of Data Processing:

- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- sending promotional emails;
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (CCTV).

What about data breaches?

It is vital to implement appropriate technical and organizational measures to avoid possible data breaches. A data breach occurs when the data for which your company is responsible suffers a security incident resulting in a breach of confidentiality, availability, or integrity. If the data breach poses a high risk to those individuals affected, then they should all be informed within seventy-two (72) hours, unless there are effective technical and organizational protection measures that have been put in place, or other measures that ensure that the risk is no longer likely to materialize.

Is our organization exempted?

If a company processes data of individuals located within the EU, it is likely that the GDPR applies. There are some exceptions to the reach of the GDPR. Some obligations of the GDPR do not apply to businesses whose activities do not center around the processing personal data when those activities do not create risks for individuals. Additionally, it doesn't extend to purely non-commercial data processed by an individual for purely personal reasons or for activities carried out in one's home. However, when an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the GDPR is implicated. Likewise, it also does not apply to the processing of personal data of deceased persons or of legal entities.

What steps would we follow as a do-it-yourself checklist to ensure compliance ourselves?

1. **What data do you have?**
   Map your business processes and examine how data flows through each department and service provider.

2. **What data do you need?**
   Identify and categorize personal data in the business process flow chart.

3. **What data must you keep and what can you delete?**
   Ask your employee or service provider that controls or processes data about their system requirements. Consider whether you process personal data of children, and ensure that notices directed at that child are "child-friendly" and if consent is relied upon, you have implemented a mechanism to seek parental consent. Also, remember to review national, state and local laws.

4. **How long must you keep it?**
   Refer to the category of data identified in your flow chart and decide how long to retain the data based on the explicit reason given in the user consent form.

5. **Who has access to the data?**
   Review your employee agreements and third-party service data processor agreements for restrictions on who has access to the data. Update agreements if data access restrictions are not expressed.

6. **Who do you share it with?**
   Draft data access policies and procedures specifying who has access to data.

7. **How secure is the data?**
   Review your security and training for gaps and process improvement.

8. **Where is your data stored?**
   Implement staff and service provider awareness training.

9. **Do you test your security?**
   Have a forensic network security expert test your network security.

10. **Have you updated your external polices?**
    Revise and publish updated terms and conditions statements as well as privacy policies on your company's websites and applications. Send out new notices to demonstrate new consents.

11. **Appoint a Data Protection Officer?**
    If your company's central purpose requires "regular and systematic monitoring of data subjects on a large scale" then you must appoint a data protection officer. You must also appoint one if you collect records of criminal convictions, or ethnicity, religious or philosophical beliefs, political opinions, trade union membership details, health, sex life, or sexual orientation data on a large scale. The EU does state that "a group" may employ one data protection officer between them, as long as the officer is readily available to each organization. The data protection officer is there to

"inform and advise" on data collection practices and monitor compliance, as well as acting as the point of contact with the data protection authority.

How Can DATH PLLC Help?
We can assist you and your company with any or all of the following:

A. CONDUCT A DATA AUDIT

Review existing data gathering/processing procedure for lawful processing and to determine if the company's current policies are still sufficient.

Determine how long personal data gathered is currently retained and the current extent of retained data to ascertain the need for its continued retention.

Also, examine whether the information can be easily accessed and/or deleted by a user who requests their information.

Conduct a data protection impact assessment to determine whether any company data practices are high risk and required additional security measures.

B. DOCUMENT ALL DATA PROCESSES

Document your privacy governance model with clear roles and responsibilities and reporting protocol to ensure privacy compliance is embedded throughout the company. For companies that may have to prove compliance with regulations such as the GDPR, it is important that they consult legal counsel that are licensed to practice commercial law in the EU and that they fully document all processes and procedures concerning staff privacy compliance training, and data collection, processing, and retention. Keep a record of your policies and practices for future reference.

C. PLAN FOR DATA BREACHES

It will be mandatory for all data breaches to be reported within seventy-two hours. Therefore, it is necessary that companies develop a plan for responding to data breaches. This plan should include a method of informing individuals of the data loss within the required time period, and also should provide for mechanism to prevent and correct a breach.

D. MONITOR DATA PERFORMANCE AND PROCESSES

Perform regular monitoring to ensure your processes are functioning properly and securely, and document the review.

E. UPDATE TERMS OF SERVICE AND PRIVACY POLICY

Data collection and retention may now only be conducted on an "Opt-In" basis. Merely passive terms of service and privacy policy are no longer sufficient. Companies should obtain the affirmative consent of individuals prior to the collection of their information. Affirmative consent includes "click-wrap" agreements, and other methods to verify user consent. It now needs to be as easy for people to revoke their consent and delete their data as it was to provide their consent and enter their data.

F. DEVELOP DATA DELETION MECHANISMS

Ensure your company has a system in place which can accommodate a withdrawal of consent to store personal data.

Companies should develop automated data deletion mechanisms so that they may remove unneeded personal data from their records, and also delete the information of individuals who have requested that their personal information be deleted.

G. HR BACKGROUND CHECKS

If your company currently conducts criminal background checks, you must now obtain explicit authorization from the individual before doing so. Local and national laws also apply restrictions to the use of employee consents to background checks.

H. REVIEW INSURANCE COVERAGE

In light of the higher fines and penalties under the GDPR, review your insurance coverage and consider whether it needs to be updated.

Conclusion

Please keep in mind that the GDPR is new, and the applications and interpretations of this regulation are forthcoming, so the legal advice contained herein may change over time. Please consult an attorney for updated advice on this memo.