DATA PROTECTION LAWS OF THE WORLD

Netherlands vs Ukraine

NETHERLANDS

Last modified 18 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

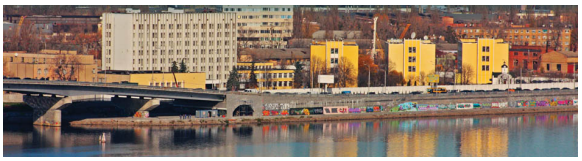
Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour* " (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Dutch GDPR Implementation Act (*Uitvoeringswet AVG*, the **Implementation Act**) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning

UKRAINE



Last modified 22 January 2024

LAW

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of June 1, 2010 (Data Protection Law) is the main legislative act regulating personal data protection in Ukraine. On December 20, 2012, the Data Protection Law was substantially amended by the Law of Ukraine, 'On introducing amendments to the Law of Ukraine’ ’On Personal Data Protection' dated November 20, 2012, No. 5491-VI. Additional significant changes to Data Protection Law were introduced by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated July 3, 2013, No. 383-VII which came into force on January 1, 2014.

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law, in particular:

- Procedure of notification of the Ukrainian Parliament's Commissioner for Human Rights on the processing of personal data, which is of particular risk to the rights and freedoms of personal data subjects, on the structural unit or responsible person that organizes the work related to protection of personal data during processing thereof (Notification Procedure)
- Model Procedure of processing of personal data (Model Procedure)
- Procedure of control by the Ukrainian Parliament's Commissioner for Human Rights over the adherence of personal data protection legislation

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg on January 28, 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows,

that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR. There is a pending legislative proposal, the Data Protection Collection Act (*Verzamelwet gegevensbescherming*), that will affect the Implementation Act on a few specific topics. For example, adjustments will be made to the definition of criminal data and the existing derogations under the Implementation Act for the processing of biometric data will be further conditioned.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data,

executed in Strasbourg on November 8, 2001 were ratified by the Ukrainian Parliament on July 6, 2010 (Convention on Automatic Processing of Personal Data) and have become fully effective in Ukraine.

In addition, data protection is regulated by:

- The Constitution of Ukraine dated June 28, 1996
- The Civil Code of Ukraine dated January 16, 2003, No 435 IV
- Law of Ukraine 'On Information' No 2657 XII, dated October 2, 1992
- Law of Ukraine 'On Protection of Information in the Information and Telecommunication Systems' dated July 5, 1994 No. 80/94 VR
- Law of Ukraine ‘On Electronic Commerce’ dated September 3, 2015, No 675-VIII
- Some other legislative acts

Furthermore, on October 25, 2022 the new Draft Law “On Personal Data Protection” No. 8153 has been submitted to Ukrainian Parliament. The said draft law is aimed at harmonizing Ukrainian data protection legislation with the standards enshrined by the GDPR and Convention 108+ and is currently expecting to be considered by Ukrainian Parliament.

DEFINITIONS

Definition of personal data

Data Protection Law defines ‘personal data’ as data or an aggregation of data on an individual who is identified or can be precisely identified.

Definition of sensitive personal data

There is no definition of ‘sensitive personal data’.

However, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offenses or conviction to criminal punishment, as well as data relating to the health or sex life of an individual.

Processing of such data is allowed if unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law *(eg,* the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are largely the same as in Article 4, GDPR. In addition, the Implementation Act defines "personal data concerning criminal law matters" as personal data concerning criminal convictions and offences or related security measures as referred to in Article 10, GDPR, as well as personal data relating to a prohibition imposed by the courts for unlawful or objectionable conduct.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the DPC in Ireland). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are

NATIONAL DATA PROTECTION AUTHORITY

Starting from January 1, 2014, Ukrainian Parliament's Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance of the data protection legislation.

regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Implementation Act.

The Dutch Data Protection Authority's contact details are as follows:

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG

Telephone number

(+31) - (0)70 - 888 85 00

Website

autoriteitpersoonsgegevens.nl

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

REGISTRATION

As of January 1, 2014, the requirement of obligatory registration of personal data databases has been abolished. However, according to new wording of Data Protection Law, personal data owners are obliged to notify the Ombudsman about personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 30 working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification to the Ombudsman:

- Racial, ethnic, national origin
- Political, religious ideological beliefs

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

- Participation in political parties and/or organizations, trade unions, religious organizations or civic organization of ideological direction
- State of health
- Sexual life
- Biometric data
- Genetic data
- Criminal or administrative liability
- Application of measures as part of pre-trial investigation
- Any investigative procedures relating to an individual
- Acts of certain types of violence used against an individual
- Location and / or route of an individual

The Notification Procedure envisages that the application for notification shall contain, inter alia the following information:

- Information about the owner of personal data
- Information about the processor(s) of personal data
- Information on the composition of personal data being processed
- The purpose of personal data processing
- Category(ies) of individuals whose personal data are being processed
- Information on third parties to whom the personal data are transferred
- Information on cross-border transfers of personal data
- Information on the place (address) of processing of personal data
- General description of technical and organizational measures taken by personal data owner in order to maintain the security of personal data

Where any of information listed above is submitted to the Ombudsman and has changed, the owner of the personal data shall notify the Ombudsman on such changes within 10 days from the occurrence of such change.

Additionally, the Notification Procedure requires the owners of personal data to notify the Ombudsman regarding the termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects, within ten days of such termination.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37 (6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

The Notification Procedure requires owners and processors of personal data that process personal data, which is of particular risk to the rights and freedoms of personal data subjects, to notify the Ombudsman on establishing a structural unit or appointing a person (data protection officer) responsible for the organization of work related to the protection of personal data during the processing. Such notification shall be made within 30 days of establishing a structural unit or appointing a responsible person.

Information regarding the said notifications of the Ombudsman shall be published on the official website of the Ombudsman.

DATA PROTECTION OFFICERS

Data owners and processors processing personal data that is of particular risk to the rights and freedoms of personal data subjects, must establish a special department or appoint a responsible person (data protection officer) to be responsible for the personal data processing matters. Other owners and processors may either establish a department or appoint a responsible person on a voluntary basis.

There are no requirements for the data protection officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule, a work permit must be obtained for him or her to hold such a position. There are no particular penalties for the incorrect appointment of Data Protection Officer.

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Implementation Act (Article 39) provides more detailed information regarding the secrecy requirement set out in Article 38(5) GDPR, by stipulating that the DPO must maintain the secrecy of any information that becomes known to him or her pursuant to a complaint by or request from a data subject, unless the data subject agrees to disclosure.

Organisations must register their DPO with the Dutch Data Protection Authority *(Autoriteit Persoonsgegevens)*. The registration form is available here.

A special email address and phone number is available for registered DPOs to contact the Dutch Data Protection Authority in case of questions with regard to the tasks of DPOs and GDPR compliance.

The contact details are as follows:

Email address: FG@autoriteitpersoonsgegevens.nl

Phone number: (+31) (0)70-8888660

COLLECTION & PROCESSING

Data Protection Principles

COLLECTION & PROCESSING

The Data Protection Law requires obtaining the consent of data subjects for the processing of their personal data. According to the Data Protection Law, the consent of the data subject means the voluntary and intentional

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract

expression of will of the data subject to the processing of personal data for the identified purposes, expressed in writing or in some other form. In the area of e-commerce, consent may be granted in the process of registration of data subjects by "ticking" a consent box during registration, provided that such a system does not allow processing of personal data before the consent is obtained. Under certain circumstances, personal data may be processed without a data subject’s consent (*eg*, legislative permission for processing of personal data, necessary to the conclusion and execution of a transaction or contract in favor of the data subject, protection of interests of data subject or data owner).

Pursuant to the Data Protection Law, as a general rule, personal data subjects shall be informed, at the moment of collection of their personal data of:

- The owner of their personal data
- The composition and content of their personal data being collected
- Their rights
- The purpose of their personal data collection, and
- The persons to whom their personal data will be transferred

However, in cases when the personal data of individuals have been collected based on the following grounds, the personal data subjects shall be informed of the above within 30 working days from the:

- Legislative permission of the owner of the personal data on the processing of personal data exclusively for the purposes of fulfilling its authorities
- Conclusion and execution of a transaction where the data subject is a party or the transaction has been concluded in favor of the data subject, which preceded conclusion of a transaction at the request of the subject of personal data
- Protection of vital interests of the data subject, or
- Need to protect the legitimate interests of the owner of personal data and third parties, except where a data subject requests that the processing of his/her personal data stops and the need to protect personal data prevails over such interest

In addition, the Data Protection Law provides the data subject with the following rights:

- To be aware of the sources of collection, location of his / her personal data, the purpose of data

- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis,

processing, the address of the owner or processor of the personal data or to obtain the said information through his / her representatives
- To obtain information in regards to the conditions of providing access to personal data, and in particular, information on third parties, to which his / her personal data are transferred
- To access his / her personal data
- To obtain a reply within 30 calendar days from the date of the receipt of his / her request, informing the individual whether his / her personal data is being processed and to receive the contents of such personal data
- To provide the owner of personal data with the reasonable request to terminate the processing of his / her personal data
- To provide a reasonable request to change or destroy his / her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate
- To protect of his / her personal data from unauthorized processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely provision of personal data, and to protect from providing invalid or discrediting information regarding the individual
- To appeal violations in the course of personal data processing to the Ombudsman or to the court
- To introduce limitations as regards rights on its personal data processing while giving the consent
- To use the means of legal protection in the case of violation of rights to personal data
- To revoke its consent on personal data processing
- To be aware of the mechanism of automatic personal data processing, and
- To be protected from the automated decision that has legal effects

The owner of the personal data can entrust the processing of personal data to the processor pursuant to a written agreement requiring that the processor process the personal data only for the purposes and in the amount permitted under the agreement. The transfer of personal data to the processor is permitted only with consent of the data subject.

provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12 (1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject

- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “ compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (i.e. opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special categories of personal data (Article 9)

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law.

Division 3.1 of the Implementation Act provides for various exceptions for the processing of different types of special categories of personal data, subject to stringent conditions. Important examples include exceptions for:

- Scientific or historical research or statistical purposes
- The processing of personal data revealing racial or ethnic origin
- The processing of personal data revealing political opinions for the performance of public duties
- The processing of personal data revealing religious or philosophical beliefs for spiritual care
- Genetic, biometric and health data

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the GDPR, except where specifically authorized under relevant Member State law.

Division 3.2 of the Implementation Act provides several exceptions for the processing of criminal convictions and offences data.

The following general grounds for exemptions for processing criminal convictions and offences data apply:

- Explicit consent by the data subject
- Protection of a data subject's vital interests
- Processing related to personal data manifestly made public by the data subject

- Processing necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
- Processing necessary for reasons of substantial public interest
- Processing necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR, and the conditions referred to in Section 24(b) to (d) of the Implementation Act have been met

Specific exceptions may apply on the basis of Article 33 of the Implementation Act, *eg,* where the processing is carried out by bodies that are responsible pursuant to law for applying criminal law, or where the processing is necessary in order to assess a request from the data subject to take a decision on him or her or to provide a service to him or her.

Child's consent to information society services (Article 8)

The Netherlands did not make use of the option to provide for a lower age limit for the processing of personal data of a child on the basis of Article 8, GDPR.

Automated Decision Making (Article 22)

The Netherlands has made use of the possibility provided by Article 22(2)(b) GDPR, and has implemented exceptions from the prohibition on automated individual decision-making. Article 40 of the Implementation Act sets out that Article 22 (1) of the GDPR does not apply if the automated individual decision-making, other than based on profiling, is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out for reasons of public interest. Examples provided by the Explanatory Memorandum to the Implementation Act concern situations where there may be automated individual decision making on the basis of strictly individual characteristics, *eg,* in the case of awarding certain allowances (*eg,* study allowances, child allowances), where there is no reason to require human intervention. In such cases, the controller must take suitable measures to safeguard the data

subject's rights, freedoms and legitimate interests. Such suitable measures will in any case have been taken if the right to obtain human intervention, the data subject’s right to express his or her point of view and the right to contest the decision, have been safeguarded.

Processing of national identification number (Article 87)

Article 87 of the GDPR sets out that Member States may further determine the specific conditions for the processing of a national identification number. The Netherlands has made use of this possibility: Article 46 of the Implementation Act sets out that a national identification number may only be processed where explicitly allowed by law, and only for those purposes stipulated by the relevant law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework), Uruguay, Republic of Korea and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses. The GDPR has removed the need which existed in some Member

TRANSFER

In accordance with Data Protection Law, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Pursuant to the Data Protection Law, such states include member states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- Unambiguous consent of the personal data subject
- Cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favor of the data subject
- Necessity to protect the vital interests of the data subject
- Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement
- Non-interference in personal and family life of the data subject, as guaranteed by the data owner

States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained;
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defence of legal claims;
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained;
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

After the European Court of Justice Decision of 16 July 2020 (Schrems II), international data transfers to countries that don’t have an equivalent level of protection can take place, if such transfers are based on the 2021 EU Standard Contractual Clauses (SCC). In addition, such in compliance with EDPB guidance, a

transfer impact assessment must be conducted in order to assess whether there are reasons to believe that the laws and practices in the third country of destination prevent the recipient from fulfilling its obligations under the SCC.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization 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 organizational measures for ensuring the security of the processing

An important security measure in line with the GDPR applicable from 1 January 2021 is that, most online payments must be completed with two-step verification. This is an obligation under the Payment Service Directive 2, the European directive for payments by consumers and businesses.

SECURITY

The data owners and processors must take appropriate technical and organizational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorized access. In this regard, owners and processors processing personal data which is of particular risk to the rights and freedoms of personal data subjects shall determine a special department or a responsible person to organize the work related to the protection of personal data during the processing thereof (other owners and processors may either establish a department or appoint a responsible person on a voluntary basis).

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain the security of personal data in all stages of their processing, including organizational and technical measures for the protection of personal data. Organizational measures shall include:

- Determination of a procedure of access to personal data by employees of the owner / processor of personal data
- Determination of the order of the recording of operations related to the processing of personal data o and access to them
- Elaboration of an action plan in case of unauthorized access to personal data, damage of technical equipment or occurrence of emergency situations, and
- Regular trainings of employees working with personal data

Personal data, irrespective of the manner of its storage, shall be processed in the way which makes unauthorized access to the data by third persons impossible.

The Netherlands have not implemented any specific regulations on the basis of Articles 24, 25 or 32 of the GDPR. In this respect, the Explanatory Memorandum to the Dutch Implementation Act explains that no general standard will be developed which sets out when an organization has fulfilled its technical and organizational security obligations. However, specific sectoral codes of conduct may be implemented which may contain further concrete standards. For example, in the health sector we see that such security standards already exist (e.g. NEN 7510, which applies as an important information security standard in the health sector).

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorized access to personal data being processed and ensure the proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners / processors processing the personal data which is of particular risk to the rights and freedoms of personal data subjects. Such structural unit or responsible person shall organize the work related to protection of personal data during the processing thereof.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The provisions regarding data breach notifications are mostly identical to Articles 33 and 34 GDPR.

Data breaches that require notification, should be notified to the Dutch DPA by completing an online form through the Dutch DPA website.

The form is available here.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

ENFORCEMENT

According to Data Protection Law, the Ombudsman and Ukrainian courts are responsible for overseeing the compliance of personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to the penalties prescribed by the law.

Violation of personal data protection legislation may result in civil, criminal and administrative liability.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The Code of Ukraine on Administrative Offenses envisages administrative liability for the following breaches of Ukrainian data protection legislation:

- Failure to notify or delay in providing notification to the Ombudsman regarding the processing of personal data or of a change to the information submitted, subject to notification requirements under Ukrainian legislation, or submission of incomplete or false information, which may lead to a fine of up to EUR 164;
- Non-fulfilment of legitimate requests (orders) from the Ombudsman or determined state officials of the Ombudsman's secretariat, regarding the elimination or prevention of violations of personal data protection legislation, which may lead to a fine of up to EUR 411;
- Non-observance of the established procedure for the protection of personal data which leads to

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

the unauthorized access of the personal data or violation of rights of the data subject, which may lead to a fine of up to EUR 411.

The criminal liability, prescribed by the Criminal Code of Ukraine, envisages fines of up to EUR 411 or correctional works for a term of up to two years, up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, or spreading of confidential information about an individual, or an illegal change of such information.

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

On the basis of Article 58(6) GDPR and in addition to the power to impose fines pursuant to the GDPR, the Dutch DPA has the power to impose an administrative enforcement order (*last onder bestuursdwang*) or an order subject to penalty (*last onder dwangsom*) to enforce obligations laid down by or pursuant to the Implementation Act.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted.

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Dutch legislation

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act (Tw). The first paragraph of Article 11.7 of the Tw is the rules for telemarketing that does not involve human intervention. These so-called automatic systems for transmitting commercial, idealistic or charitable communications may only be used if the consumer has given his prior consent. As of 1 July 2021, the Dutch

ELECTRONIC MARKETING

The Law of Ukraine ’On Electronic Commerce’ dated September 3, 2015 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce (i.e. electronic messages in any form, the purpose of which is to promote, directly or indirectly, goods, works, services, business reputation of a party engaged in a business or self-employed professional activity). In particular, commercial electronic messages shall be distributed only subject to the consent given by individual to whom such messages are addressed. At the same time, commercial electronic messages may be distributed to an individual without his / her consent only if such individual has an option to object to receiving such messages in future.

In addition, commercial electronic messages shall satisfy the following criteria:

- Commercial electronic messages shall unequivocally be identified as such.
- The recipient shall have easy access to information regarding the person sending the message as stipulated by the Law of Ukraine ‘On Electronic Commerce’, in particular:

Telecommunications Act changed. As a main rule, also for telemarketing with human intervention, the opt-in system will be used.

New Legislation

The ePrivacy Regulation is a proposed regulation governing the use of electronic communication services within the European Union and is intended to replace the Directive on privacy and electronic communications (Directive 2002/58/EC). In addition to the GDPR, the ePrivacy Regulation represents a core element of EU-level data protection. On 10 February 2021, the Council of the European Union ('the Council') published a new legislative proposal, thereby launching negotiations between the Council, the European Parliament and the European Commission.

In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

- full name of legal entity / individual and place of registration / residence;
- email / website of the online shop;
- registration number or tax ID number / passport details (for individuals);
- license data (in case if it is mandatory under the law);
- inclusion of taxes in calculation of the price of goods / services; and
- price of delivery of goods (in case if delivery is performed).

- Commercial electronic messages regarding sales, promotional gifts, premiums and etc. shall be unequivocally identified as such and the conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

In addition, under the Law of Ukraine "On Electronic Communications" dated December 16, 2020, end-users may use telephone numbers or other network subscriber identifiers obtained by any person in the course of selling goods or providing services to send advertisements for the purpose of selling goods or services only with the consent of the end-user, including in electronic form, and if the recipient is given the opportunity to refuse the use of his or her data at any time, free of charge, in a simple and understandable manner.

Furthermore, distribution of spam is generally prohibited. Spam is defined quite broadly as more than five messages (electronic, text and / or multimedia messages) sent to one recipient without the recipient's prior consent.

ONLINE PRIVACY

Traffic Data

Traffic Data is regulated in Article 11.5 of the Tw. Traffic Data held by a public electronic communications services provider (CSP) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

ONLINE PRIVACY

There is no specific legislation regulating online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involve the processing of personal data.

- It is being used to provide a value added service; and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service (subject to consent)
- Market research (subject to consent)

Location Data

(Traffic Data not included) – Location Data is regulated in Article 11.5a of the Tw. Location Data may only be processed:

- If such data is being processed in anonymous form; or
- With informed consent of the individual.

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. The Authority for Consumers and Markets (ACM) is entrusted with the enforcement of Article 11.7a of the Tw. In addition, in relation to cookie compliance all privacy requirements from the GDPR must be taken into account. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Dutch GDPR Implementation Act.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt-in) and needs to clearly and unambiguously inform the user about these cookies (purpose, type of cookie, etc.). Please note that the website operator is not entitled to refuse users access to its website(s) if no consent is given. The requirement to obtain prior consent from a user does not apply in case of functional cookies (e.g. to enable web shopping carts or language choices) and analytical cookies that have little or no impact on the user's privacy (e.g. for testing the effectiveness of certain banners / pages with the aim to improve the website). In such case, the website operator still needs to inform the website visitors about the cookies.

The information collected through cookies are considered personal data, unless the party that places the cookies can prove otherwise.

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines of up to EUR 900,000 per violation. In some cases, the fine may be even higher and amount to a percentage of the total annual turnover. In case of violation of the GDPR and the Dutch GDPR Implementation Act, the Dutch Data Protection Authority can impose fines up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

KEY CONTACTS

Richard van Schaik
Partner
T +31 20 541 9828
richard.vanschaik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KEY CONTACTS

Natalia Kirichenko
Partner
Kinstellar Ukraine LLC
T +380 (44) 490 9575
natalia.kirichenko@kinstellar.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.