КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

LEGAL GROUNDS FOR LAWFUL PERSONAL DATA PROCESSING

This informative document aims at supporting the practical implementation of the Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). It is not obligatory and comprehensive. The analysis reflects the general personal data processing, but not the special categories of data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as, personal data relating to criminal convictions and offences.

The personal data processing by controllers in the public and the private sphere is lawful, if any of the following alternative and equal grounds applies:

- consent;
- performance of contract;
- legal obligation;
- vital interests;
- public interest/official authority;
- legitimate interests.

The listed grounds order does not give advantage or more importance of one over the other.

The duplication of legal grounds for the same personal data processing operation is inadmissible- the data processing ground should be clearly determined and the only valid, i.e. no overlapping of two or more processing grounds for the same activity should occur.

CONSENT

The data subject (natural person to whom the data relate) has given consent for his/her personal data processing for one or more specific purposes.

In order to be legitimate, the consent should simultaneously correspond to every one of the determined criteria:

- to be freely given- not under pressure or threat of adverse consequences (e.g. higher service price, inequality in the relations with the controller, such as, as a rule are the relationships between employer and employee/official);
- to be specific- separate consent for every specifically determined purpose, and when relevant- for specific personal data category;
- to be informed- given on the basis of full, clear and easy understandable information;
- to be unambiguous- is not extracted or suggested on the ground of the individual's other statements or actions;
- to be explicitly stated or clearly affirmative action- e.g. ticking a box by pressing a certain button and etc.

The controller is obliged to demonstrate the data subject's consent legitimacy.

General consent validity test is the check, whether the personal data processing will cease when the consent is withdrawn.

Important! When data are processed on any of the other grounds, the consent is not necessary and invalid and demanding it will be considered as excessive data processing.

Example

A controller, which is a state authority, offers administrative service, requiring personal data processing. Requesting consent for the provision of service, stemming from the authority's powers and administrative competences is inadmissible. For example, by consent validity test will be established that the consent for administrative services provision cannot be withdrawn- i.e. by definition, the public authorities process data on other grounds.

Important! The controller has to guarantee that the consent can be withdrawn by the data subject, as easy as, it is given and at any time.

Example

Data controller offers music application and requests consent from the citizens to process their musical preferences in order to propose personalized offers.

Important! Considering that the children are more vulnerable society group, Art. 25c of the Personal Data Protection Act foresees enhanced protection for persons under 14 years and the consent given by them is only valid, if given by the child's parent or guardian.

References:

Article 6, as well as Recital (40) of Regulation (EU) 2016/679;

Article 7, as well as Recitals (32), (33), (42), (43) of Regulation (EU) 2016/679;

Guidelines on consent under Regulation (EU) 2016/679.

PERFORMANCE OF CONTRACT

The processing is necessary for **the performance of contract** to which the data subject is party or in order to take steps at the request of data subject prior to entering into a contract (pre-contractual relations).

The processing is lawful, if:

- the controller has contract with the individual and has to process his/her data in connection with the performance of contractual obligation.
- the controller has no concluded contract with the individual, but are undertaken pre-contractual actions on data subject's behalf (exam. provision of personalized offer for specific product/service).

Example

A company sells products on-line. It processes data necessary for the undertaking of actions on individual's behalf before concluding contract and for performance of contract. Thus, it can process name, delivery address, credit card number (when paying by card) etc.

When the data subject buys on-line, the controller processes the individual's address in order to deliver the products.

That is necessary for the performance of the contract.

Important! The contract's form can be written, as well as oral. In all cases, the controller has to proof the existence of the ground.

Example

By concluding mediation contract for property purchase, the agency, with which you work, processes personal data for the contract performance purposes and accordingly, it is not necessary to give consent for the processing, resulting from every property inspection or at any stage of the deal/trade.

References:

Article 6, as well as Recital (44) of Regulation (EU) 2016/679;

LEGAL OBLIGATION

The processing is necessary for compliance with a **legal obligation** to which the controller is subject.

The general processing purpose should be in compliance with legal obligation, foreseen specifically in the national or EU legislation.

The controller should identify the obligation in question either by referencing to specific legal provision or by using other procedure and pointing the source.

Examples

If you are an employer in order to organize your employees' social security, by law, you are obliged to submit personal data (e.g. employees' incomes) to the relevant state authority.

Financial institution identifies its potential or current client via ID document copy (including ID card) following a legal obligation, set in the Measures against Money Laundering Act.

The condominium manager, in building with such regime, processes owners and occupants' personal data in order to fill and keep updated the home book following the requirements, set in the Condominium Management Act.

References:

Article 6, as well as Recitals (41), (45) of Regulation (EU) 2016/679;

VITAL INTERESTS

The processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.

Important! In this case, vital interest means an interest related to the data subject's life and health!

This legal ground is applicable to the highest degree for emergent medical help, in cases, when personal data must be processed for medical purposes, but the individual is in no condition to give consent for the processing.

It is unlikely, the personal data processing related to planned medical activities to be based on individual's vital interests. The personal data processing of one individual in order to protect the vital interests of another person or persons is also very limited. Exceptions also exist: for example, by processing parents personal data (such as: family burden), when necessary, in order to protect the child's vital interests.

Examples

The hospital treats a patient after severe road incident; the hospital does not need his/her consent in order to process ID card data for verifying, whether this person exists in the hospital data base, to find previous illnesses or contact his/her relative.

Important! In the most cases, the protection of individual's vital interest will arise from the individual's health data processing. So these data are special categories of data, meaning that when processing them, the controller should take into account the conditions for special categories of data processing, set in Article 9 of Regulation (EU) 2016/679.

References:

Article 6 of Regulation (EU) 2016/679;

PUBLIC INTEREST/ OFFICIAL AUTHORITY

The 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.

The controller should document the performance of task carried out in public interest or the exercise of the official authority in order to prove the personal data processing ground (accountability principle).

For the accountability purposes, the personal data controllers/processors should determine the relevant tasks, functions or competences in specific legal texts.

Every organization exercising official authority or carrying specific task in public interest can refer to this ground. The emphasis is on the nature of the function not on the organization.

Example

In general, the state authorities, including the local government, process lawfully personal data on the ground of exercising official authority and not on the basis of consent.

Important! The data subjects' erasure and portability rights are not applied, if the processing is based on performing task in public

interest or exercising official authority. The individuals can, however, object to the specific processing.

References:

Article 6, as well as Recitals (41), (45), (50) of Regulation (EU) 2016/679;

LEGITIMATE INTERESTS

The 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.

The personal data controller/processor should document its personal data processing decision taken on the legitimate interest ground, demonstrating compliance with Regulation (EU) 2016/679 (accountability principle). The data subjects should be informed in details about the reference to this legal ground.

In order to protect the individuals' rights, the personal data controller/processor should apply the so call "proportionality test", which can contain:

- Purpose: is legitimate interest pursued? (necessary check for existence of other personal data processing legal ground)
- Necessity: is the personal data processing necessary for the achievement of this purpose? (is it possible to achieve the purpose without personal data processing or by processing less data).
- Proportionality: does the individuals' interests override the controller's legitimate interest? (is the level of interference in the data subject's privacy comparable with the controller's legitimate interest importance).

Examples

Your organization guarantees its network security by monitoring the employees' computer devices. The organization can process personal data for that purpose only, if the chosen method, limits, as little as possible, the employee's right of privacy and personal data, e.g. via limiting the certain websites accessibility. In all cases, the employees and interested parties should be informed about this.

Insurance company process personal data for insurance fraud prevention purpose. The personal data processing is on the ground of controller's legitimate interest.

References

Article 6, as well as Recitals (47), (48), (49) of Regulation (EU) 2016/679;

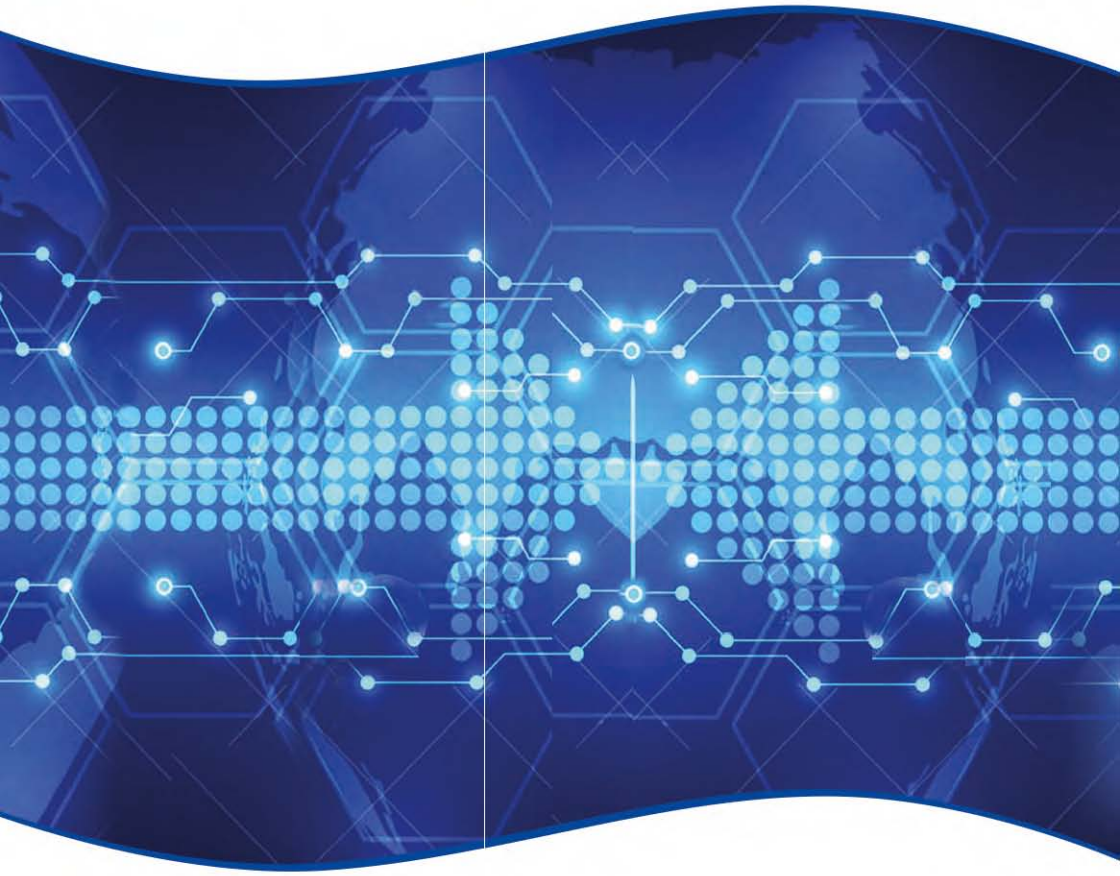
INDIVIDUALS' RIGHTS IN RELATION TO THEIR DATA PROCESSING GROUNDS

Some data subjects' right under the GDPR are applied only when the processing is carried out on specific legal grounds. The table below provides information, which rights could be exercised, when personal data are processed following different legal grounds.

	consent	performance of a contract	legal obligation	vital interests	public interest/ official authority	legitimate interests
Right to information						
Right of access						
Right to rectification						
Right to erasure ("Right to be forgotten")						
Right to restriction of processing						
Right to data portability						
Right to object						
Rights to automated individual decision-making, including profiling						

* Green- fully applicable; yellow- partially applicable; red- inapplicable.

It should be taken into account that other requirements or limitations with regard to some of the above-mentioned data subjects' rights can exist, but as a first step, the controllers should examine which rights can be applied, when fulfilling their personal data protection obligations. Also, the individuals always have the right to object to their personal data processing regardless of the legal ground applied.



КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

Commission for Personal Data Protection
2 Prof. Tsvetan Lazarov Blvd., Sofia 1592
E-mail: kzld@cpdp.bg
Web-site: www.cpdp.bg