

LEGITIMATE INTEREST Approved 15.05.2020 This guide explains how to apply the legitimate interest provided for in Article 6(1)(f) of the General Regulation on Personal Data Protection 2016/679 as a legal basis for data processing.	2
Table of contents	
1. Abbreviations used	2
2. Legitimate interest as a legal basis for processing personal data	3
3. Demarcation from other bases of personal data processing	3
3.1. For the introduction of measures prior to the conclusion of the contract in accordance with the data subject's request (IKÜM art. 6 paragraph 1 point b)	4
3.2. To fulfill the contract (IKYM art. 6 paragraph 1 point b)	4
3.3. In case of breach of contract, to prepare legal claims (IKÜM art. 6 paragraph 1 p f).....	5
3.4. In order to fulfill the legal obligation of the controller (IKÜM art. 6 paragraph 1 point c)	5
4. Three-stage evaluation of the legitimate interest	6
4.1. Legitimate interest of the controller or a third party	6
4.2. Interests and rights of the data subject	7
4.3. Weighing/balancing	8
4.4. Additional safeguards and reconsideration	9
5. The data subject's right to object	10
Transparency, impact assessment	11
Remember!	
Abbreviations used IKS – Personal Data Protection Act, 12.12.2018. a - RT I, 04.01.2019, 11 IKÜM - General Regulation on Personal Data Protection 2016/679, 27 April 2016 EAKN - European Data Protection Council, which was established by the General Regulation on Personal Data Protection and replaces the previous working group formed on the basis of Article 29 of the Personal Data Protection Directive 95/46/EC . Ensures uniform application of data protection rules by issuing guidelines and instructions. A29 working group - a working group operating on the basis of Article 29 of the Personal Data Protection Directive 95/46/EC until May 25, 2018, which prepared positions and instructions on data protection issues. TLS - Employment Contract Act, 17.12.2008. a – RT I 2009, 5, 35; RT I, 19.03.2019, 94 VÜS - Law of Obligations Act, 26.09.2001. a - RT I 2001, 81, 487; RT I, 08.01.2020, 10 ESS - Electronic Communications Act, 08.12.2004. a – RT I 2004, 87, 593; RT I, 08.01.2020, 4 1 Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016, on the protection of natural persons in the processing of personal data and on the free movement of such data. Online: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679 (23.03.2020).	
3 Legitimate interest as the legal basis for personal data processing IKÜM art 6 paragraph 1 p f: "Personal data	

processing is necessary in the case of a legitimate interest of the data controller or a third party, unless such interest is outweighed by the interests of the data subject or the fundamental rights and freedoms for which personal data must be protected, especially if the data subject is a child. "To use it, it is necessary to compare the legitimate interests of the controller or third parties receiving data with the interests or fundamental rights of the data subject, the result of which determines whether the referenced provision can be used as a legal basis for processing. The provision of legitimate interest was also outlined in the personal data protection directive 95/46/EC art 7 p-s f, but still it was not adopted into Estonian law as a general rule. On April 14, 2016, the European Parliament approved the General Data Protection Regulation (hereinafter GDPR), which replaced the former data protection directive. IKÜM is directly applicable and together with the new Personal Data Protection Act (hereinafter IKS) replaces the previous Personal Data Protection Act adopted in 2007. In the case of special types of personal data, there is no such basis in Art. 9 of the IKÜM, but the preparation, submission or defense of legal claims is still allowed in the case of special types of personal data. The public sector cannot rely on this basis when processing personal data (the last sentence of art. 6, paragraph 1 of IKÜM states that p-i f cannot be used if the data is processed by a public sector institution in the performance of its tasks), point 49 of IKÜM points out that the institution could still rely on it in administrative activities not related to the main activity, e.g. management of the institution, security of the building and information systems (it is known that previously public sector institutions relied on a special provision of the IKS regarding security cameras, which no longer exists). At the same time, both the Public Information Act and the Cyber Security Act oblige institutions to ensure the security of information assets and databases, and for this purpose, one of the possible measures in the implementation of ISKE is the use of video surveillance. Therefore, in the case of institutions, the use of video surveillance can also be based on Article 6(1)(c) of the IKYM. In the case of the first five grounds provided for in Article 6(1) of the IKÜM, the legality of data processing is based on the data subject's consent, contractual orders, statutory obligation or other specific reason defined in the legislation. However, on the basis of the legitimate interest provided for in Article 6(1)(f), data processing is legal only if a thorough consideration of the interests of the parties has been correctly carried out, from which a conclusion on the justification of data processing can be clearly seen. We will try to explain how to do this with this guide. Demarcation from other grounds for personal data processing Contract, consent and legitimate interest can all exist side by side within the framework of a relationship with the same data subject. Therefore, for each processing operation, it is necessary to clearly distinguish and determine on which legal basis the specific data processing takes place. 2 Directive 95/46/EC of the European

Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (repealed). Online:

<https://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX%3A31995L0046> (23.03.2020). 4 In the following subsections, we

highlight the most typical examples of defining the legal basis of data processing related to contractual relationships. 3.1. For

the introduction of measures prior to the conclusion of the contract in accordance with the data subject's request (IKÜM art. 6

(1) p. b) Art. 6 (1) p. b can be relied on only on the assumption that specific measures are introduced at the request of the data

subject and not at the initiative of the data controller or a third party. For example, an individual asks a company to send him

an offer for a specific product (this also includes the right to retain the data subject's address and information about the request

for a limited period of time). On the other hand, detailed background checks, for example in a situation where the insurer

processes the applicant's health data before providing health or life insurance, cannot be considered a necessary action

performed at the request of the data subject. The insurance provider has the right to request personal data from the Insurance

Activities Act, i.e. in this case personal data will be processed for the purposes and on the basis provided for in the law (the

legal basis is IKÜ Article 6(1)(c)). It is also legitimate from the entrepreneur's point of view to ask customers to provide

essential personal data and to prove their identity when concluding a contract. At the same time, making and keeping a copy of

an identity document, as a rule, goes beyond what is necessary to fulfill the contract, and the legal basis for such an activity

may instead be a legal obligation (e.g. § 21 of the Prevention of Money Laundering and Terrorist Financing Act - identification

of a natural person, the underlying documents and data collected about the customer). Also, checks of payment irregularities,

which are carried out before issuing a loan to a person, are not based on the request of the data subject (IKÜM art. 6

paragraph 1 p. b), but on the basis of legitimate interest in order to make sure of the reliability of the future contracting partner

(IKÜM art. 6 paragraph 1 p f). The need to check payment disorders may also arise from the banks' statutory obligation to

check the credit applicant's ability to pay (IKÜM art. 6 paragraph 1 point c). The justification for the processing of personal data

(i.e. the existence of an acceptable legitimate interest) in pre-contractual relations may result from special laws, e.g. regarding

the justification for the processing of personal data directly related to the performance of work duties (i.e. the existence of an

acceptable legitimate interest), see more specifically the special laws, e.g. provisions concerning pre-contractual negotiations

TLS § 11, VÖS § 14. 3.2 . To fulfill the contract (IKÜM art. 6 paragraph 1 point b) Processing must be objectively necessary to

achieve the purpose stipulated in the contract or to fulfill a specific contractual obligation. The fact that the contract contains a

general clause about the processing of personal data (e.g. direct marketing or transfer of debt data to the default register) does not automatically mean that the processing of personal data is necessary for the performance of the contract. EAKN explains that if there are realistic less intrusive alternatives to achieve the purpose of the contract, the processing operation is not necessary.³ According to the sales contract, the processing of personal data is allowed, for example, to deliver the goods, but not for further profiling of taste and lifestyle preferences based on clicks made by the customer on the website and purchased items. In the case of profiling, it is possible to rely on the basis of legitimate interest under certain conditions (provided that it is proportionate). Entitled 3 EAKN Guidelines 2/2019 on the processing of personal data on the basis of Article 6(1)(b) of the General Regulation on the Protection of Personal Data in connection with the provision of internet-based services to data subjects, p 2.4. 5 interest cannot be relied upon if an automatic decision is made about the data subject along with profiling (IKÜM art. 22). In the case of employment relationships, it is also not possible to monitor the employee's Internet use, e-mails or telephone use, or check employees in any other way for the purpose of fulfilling the employment contract. This is where the close connection and the need for delineation is manifested - checking the employee is closely related to the obligations arising from the employment contract, but at the same time, checking is not necessary to fulfill the employment contract. At the same time, checking the work duties of employees may be permitted if the employer has a legitimate interest. Fraud prevention, which may include, among other things, customer monitoring and profiling, is another typical area where, given the purposes of personal data processing, there may likely be an excessive excess towards data subjects, i.e. activities that clearly exceed what is necessary to fulfill the contract. Recital 47 of the IKÜM indicates that the processing of personal data strictly necessary to prevent fraud is also a legitimate interest of the controller concerned. 3.3. In order to prepare legal claims in the event of a breach of contract (IKÜM art. 6 paragraph 1 p f) the Article 29 working group explained in its opinion 06/2014,⁴ that the legal basis "contract performance" is suitable as long as the processing is related to the normal performance of the contract. However, the processing of the data subject's basic data - such as name, address and details regarding unfulfilled contractual obligations - for sending official reminders must still be considered as processing of personal data necessary for the performance of the contract. If an incident occurs during the performance of the contract or the contract is not performed and it is necessary to start preparing legal requirements, such processing will no longer take place within the scope of the normal performance of the contract and therefore it cannot be based on IKÜ Article 6(1)(b). Such an example can be given when collecting a debt through external service providers (collection companies) or suing a customer who has not paid for the

service. In this case, the basis of "legitimate interest" should be used (or, in the case of special types of personal data, Art. 9(2)(f) IKÜM). 3.4. In order to fulfill the legal obligation of the responsible processor (IKÜM art. 6 paragraph 1 point c) IKÜM article 6 paragraph 1 p-s c provides the legal basis for situations where processing is necessary to fulfill the legal obligation of the responsible processor. This may apply, for example, if employers have to submit salary data of their employees to the social security institution or the tax authority, or if financial institutions are obliged to report suspicious transactions to the competent authorities according to anti-money laundering regulations. Recital 45 of the IKÜM specifies that if processing is carried out in accordance with the fulfillment of the legal obligation of the controller, the basis of processing should be provided in the legislation of the Union or Member State. The rule must be taken into account that the processor of personal data must not have a choice whether to fulfill the obligation or not. Therefore, the basis of legitimate interest should not be relied on here either. Those situations must also be delineated when a special law requires the disclosure of personal data to the public (with the aim of ensuring transparency) and the personal data processor's own desire to disclose personal data for the purpose of ensuring transparency and accountability. The latter can be done under the IKÜM legitimate interest provision. For example, the Board of Health discloses the data of healthcare workers because the law requires it, but the hospital can disclose the names of doctors on its website based on a legitimate interest (the need to make the offered service transparent for the patient).

4 Opinion 06/2014 on the concept of legitimate interests of the data controller within the meaning of Article 7 of Directive 95/46/EC in order to ensure the transparency and controllability of relations between drug manufacturers and doctors. 6, for example, pharmaceutical manufacturers wanted to disclose the names of healthcare workers who have been paid or given other bonuses.

Three-stage assessment of legitimate interest In Article 6(1)(f) of the GDPR, three conditions are prescribed, all of which must be met in order for the processing of personal data to be permitted: 1) the controller or the third party or third parties receiving the data have a legitimate interest, 2) the processing of personal data is necessary for the realization of a legitimate interest, 3) the interests of the controller or a third party receiving the data are not outweighed by the fundamental rights and freedoms of the protected data subject. Its evaluation is carried out according to a three-stage scheme:

Level I - interests of the personal data processor or third parties and their importance
Level II - rights and interests of the data subject and importance
Level III - weighing of conflicting interests - preliminary assessment + additional protective measures if necessary final assessment

If the data controller has an interest in any personal data against processing, this does not automatically mean that he can rely on the basis of legitimate interest. The justification of the controller's interest is only a

starting point, i.e. one of the elements that must be analyzed, and whether the basis of legitimate interest can be relied on depends on the result of the balancing. Convincing whether the provision of legitimate interest can be relied on is the responsibility of the data controller, who should carry out the consideration in a transparent manner and be able to justify his decision. In the event of a possible extensive and intensive interference resulting from data processing, it may be necessary to prepare a written data protection impact assessment (ICÜM art. 35; read more in the general manual of the Personal Data Processor). The legitimate interest must be assessed periodically. Due to circumstances that have changed over time, the legitimate interest may end or the interests of the data subject may prove to be more important.

4.1. Legitimate interest of the controller or a third party

The proposed data processing may be in the interest of the controller (e.g. the employer, the company itself), a third party (e.g. a company requesting debt data) or the general public, i.e. an unlimited circle of persons (e.g. the entire public in the case of publication of a newspaper article in an online publication). Legitimate interest may include broader interests of the personal data processor, both significant and minor, i.e. only when such interests are balanced with the interests and fundamental rights of the data subject, a more limited approach and substantive analysis must be applied. The A29 working group (see reference 4) has outlined the most typical interests in the guideline (they do not in any way assess whether or not the interests of the controller outweigh the interests and rights of the data subjects in the balancing process):

- Exercise of the right to freedom of speech or information, including in the media and the arts (there are special provisions on this in Sections 4 and 5 of the IKS);
- conventional direct marketing and other types of marketing and advertising activities;
- ensuring compliance with legal requirements, including debt collection through out-of-court procedures;
- 7 □ prevention of fraud or misuse of services;
- monitoring workers for safety or management purposes;
- breach reporting mechanisms;
- physical security, IT and network security;
- data processing for historical, scientific or statistical purposes (there is a special provision for this in Section 6 of the IKS);
- processing for scientific research (including market research, also a special provision in IKS § 6)

The legitimate interest must be: legal (illegal desire is not protected); sufficiently clearly formulated (specific); real and current (not speculative). Controllers who are part of a group may have a legitimate interest in transferring personal data of customers or employees within the group for internal management purposes. The general principles of transferring personal data to an enterprise located in a third country within the group remain the same (see also Chapter V of IKÜM). In terms of direct marketing, it must be clarified that direct marketing via e-mail or SMS can only be done with the prior consent of the person (except for the exception of ESS § 1031 (3) in the case of a previous customer relationship). In the

context of direct marketing based on legitimate interest, we can talk about profiling and, for example, targeted advertising on internet pages. Surveillance devices (so-called security cameras) are a classic example of personal data processing based on legitimate interest. On the basis of the previously valid directive⁵ (which, unlike the regulation, was not directly applicable), the IKS provision was developed, specifically § 14 paragraph 3, which allowed the use of monitoring devices for the protection of persons or property. IKÜM, as a directly applicable legislation, and in connection with it, IKS, which entered into force on 15.01.2019, no longer allows such a legal basis, which means that tracking devices can only be used on the basis of the legitimate interest stipulated in IKÜM. It is true that the exception is an obligation imposed by law, e.g. casinos due to § 37 subsection 14 of the Gambling Act. You can read more about surveillance devices in the Data Protection Inspectorate's instructions on the use of cameras.

4.2. Interests and rights of the data subject

The provision refers to the interests of the data subject as well as the fundamental rights and freedoms. This is to ensure greater protection for data subjects. That is why IKÜM art. 6 paragraph 1 p f requires that the interests of data subjects must also be taken into account, not only their fundamental rights and freedoms. All relevant interests of the data subject must be taken into account. In addition, it is important to note that unlike the interests of the data controller, the word "legitimate" is not used here in front of the interests of data subjects. Both positive and negative consequences must be taken into account when assessing the impact of processing. These may include possible future decisions or actions taken by third parties and situations where the processing may result in the exclusion or discrimination of individuals, damage to reputation or, more generally, situations where there is a risk of damage to reputation, bargaining power or autonomy. In addition to the harmful consequences that can be specifically foreseen, the wider emotional impact such as irritation, fear and worry that may result from the data subject no longer having control over his personal data ⁵ See reference 3 8 or realizing that that they are or may be abused or compromised, for example through online disclosure. Even the rights and interests of individuals involved in illegal activities should not be disproportionately violated. For example, an individual who has committed theft in a grocery store may still consider his own interests to be more important than those of the store owner in a situation where the store owner publishes his picture and home address on a billboard in the store and/or on the Internet. For example, within an apartment association, the members of the association have the right to know who owes the association, but this information cannot be publicly posted in the stairwell. E.g.: If a person crosses the road in a place not designated for this, thereby causing a dangerous traffic situation, publishing a photo taken by an eyewitness, for example, in a social media group of traffic hooligans, may excessively violate the rights of

the person. 4.3. Weighing/balancing Having described the interests of the parties, it is necessary to assess whether the impact caused by the processing of personal data on the data subject is proportional to the requested purpose. The encroachment of fundamental rights and freedoms is excessive if there is another means that helps to achieve the set goal just as well, but does not encroach on the rights of the person as strongly. In Estonian legal practice, a three-part test of proportionality has been implemented to assess this: The remedy is proportional only if it is suitable (suitable), necessary and moderate for achieving the set goal. A remedy is appropriate if it facilitates the achievement of the goal of the restriction. A remedy is necessary when the goal cannot be achieved with another, less burdensome remedy. In order to assess moderation, the importance of the interests of the data subject and the extent of the infringement of rights must be considered on the one hand, and the importance of the purpose of the processing on the other hand. These criteria are also supported by the principles of personal data processing outlined in Art. 5 of the IKÜM - primarily purposefulness and minimality, which must also be fully followed when processing personal data on the basis of legitimate interest. Fair processing, quality (i.e. redundancy must be excluded), correctness (i.e. personal data must be correct and, if necessary, updated, corrected or deleted), storage limitation (the data subject must be able to be identified only as long as it is necessary for this purpose) are no less important. fulfillment for which personal data is processed) and security principles (must be protected against unauthorized or illegal processing, including against loss, destruction, damage by applying appropriate technical or organizational measures). Personal data may be processed only in the case and to the extent that it is really necessary to achieve the specified goals and provided that there are no less intrusive measures to fulfill this goal. The cost of an alternative measure that infringes on privacy less or not at all cannot be the sole determinant. For example, the employer's goal is to ensure the security of property at the workplace, so the employer decides to install cameras in the workplace. At the same time, the continuous monitoring of employees during the working day can be excessive, so the employer must also consider whether the remedy is really necessary or if it is possible to implement other measures (e.g. security gates, security elements on the goods) or change the angle of the camera in such a way that it only points to the goods shelf. 9 When weighing interests, the legitimate interest of the controller or a third party is placed on one scale, and the interests and rights of the data subject on the other. If the impact on the data subject is very large, while the weight of the personal data processor's interests is low, a firm decision can be made: the interference is disproportionate and the planned personal data processing is not allowed. The more intense the infringement of the data subject's rights, the more compelling the reasons justifying it must be. How to assess the importance of the interests of one

and the other side? The A29 Working Group notes that cultural and social expectations, even if not directly reflected in legislation, can also be important and help tip the scales in one direction or another. The more explicitly the law, other legal regulations (whether they are binding on the controller or not) or the relevant society, even without a specific legal basis, generally recognize that controllers can take measures and process data to realize a certain interest, the more weighty such legitimate interest is in balancing. When assessing the impact on the data subject, the following are taken into account: type of personal data, status of the data subject (child, vulnerable part of the population, elderly), method of personal data processing, reasonable expectations of the data subject, whether and for what purpose it has been disclosed in advance, whether a large amount of personal data is processed or whether it is merged with other personal data (e.g. profiling), whether less intrusive methods enable the controller's goals to be achieved. The reasonable expectation of the data subject, i.e. that his personal data will not be processed in a way that he cannot reasonably foresee, is also relevant for consideration. The balance of power between the data subject and the controller is also important. Depending on the specific circumstances and whether the controller is an individual, small or large organization, the personal data processor may be in a stronger or weaker position in relation to the data subject. In labor relations, the employee and the employer are not on an equal footing. In the case of personal data previously disclosed (whether by the data subject himself or by third parties), it is important to emphasize that the provision of legitimate interest does not allow re-disclosure without restrictions. Although the public availability of personal data can be a factor to be considered in certain situations, it is still necessary to see for what purpose and how (to a large number of people, how to find) the original disclosure was made and whether the re-disclosure is compatible with this. Also, whether it was reasonable to expect that personal data may be used for other purposes in the future (e.g. for research or transparency and accountability purposes).

4.4. Additional protective measures and new consideration

The consideration described in the previous point must give an answer as to how important the interests of either side are and how big the impact is on the interests and rights of the data subject. In the adjacent figure, it can be concluded from the result of the weighing that the interests of both parties have a similar weight: Interests and rights of the data subject Legitimate interests of the processor of personal data

10 In case of equal weight, the legitimate interest cannot be relied on. It is therefore necessary to implement additional safeguards to reduce the impact on data subjects. It should be kept in mind that the additional protective measure does not mean statutory obligations. The A29 working group has outlined examples of possible additional safeguards: strict limits on the amount of personal data collected, immediate deletion of personal data after use, technical and organizational

measures to ensure separation by function, appropriate use of anonymization techniques, aggregation of personal data and privacy-enhancing technology, and in addition greater transparency, accountability and opportunity in processing opt out of participation. Regarding the use of pseudonyms and encryption, the working group emphasizes that the fact that the data is not directly identifiable does not affect the legality of processing - it should not be considered as legalizing illegal processing. For example, an Estonian company that resells vehicles has found that its legitimate interest is the development of services and the measurement of customer satisfaction within the framework of the provision of services and the sale of goods. If a company wants to order a survey from a research company, it has a legitimate interest as the responsible data processor, and for this purpose, the research company can send a customer survey invitation to the customer's e-mail address on behalf of the company. The processed data composition is minimal - the customer's e-mail address. However, the company has implemented an additional protection measure and added an opt-out link to the survey invitation so that the customer will not receive such invitations in the future. The privacy policy is published on the company's website, where such legitimate interest is outlined. The data subject's right to submit an objection IKÜM art 21 paragraph 1 stipulates the data subject's right to submit objections at any time to the processing of personal data concerning him, which has taken place on the basis of legitimate interest, including profile analysis based on this provision. Upon receiving an objection, the data controller may not further process personal data, unless it proves that personal data is being processed for a valid legitimate reason that outweighs the interests, rights and freedoms of the data subject, or if the situation concerns the purpose of preparing, presenting or defending a legal claim. The data subject has the right to object based on his specific situation, i.e. to point out why, from his point of view, the processing of his personal data is excessive. In this case, based on the objection, the controller must reassess the situation of this person and prove that he also has a valid and legitimate reason considering the specific case. The A29 Working Group has emphasized that in the event of an objection, the controller cannot simply refer to the initial legitimate interest assessment or the privacy policy. If the data controller cannot prove that he can still rely on his legitimate interest, taking into account the situation of the specific data subject, the data subject has the right to demand the termination of further data processing and the deletion of personal data. (see IKÜM art. 17 paragraph 1 point c). The data subject can already submit a claim to this effect together with an objection. Interests and rights of the data subject Legitimate interests of the processor of personal data become more weighty with additional protective measures 11 If an activity related to direct marketing took place based on the provision of legitimate interest, the data controller does not have the opportunity to evaluate

or justify anything further. In case of objection by the data subject, the processing must be terminated (ICYM art. 21, paragraph 3).

3). Transparency, impact assessment

The principle of fair and transparent processing requires that the data subject is informed of the performance of the personal data processing operation and its purposes. The principle of transparency means that information addressed to the general public or the data subject is concise, easily accessible and understandable, and clearly and simply formulated, and visualization should also be used additionally if necessary. The data protection conditions intended for the data subject should clearly distinguish between the legal bases of data processing and data composition according to different data processing purposes. A data protection impact assessment must be carried out by all personal data processors who, given the nature, scope, context and purposes of their personal data processing, are likely to pose a high risk to people (see IKÜM art. 35). If the data protection impact assessment shows that as a result of the processing, in the absence of protective measures to mitigate the threat and security measures and mechanisms, a great threat to the rights and freedoms of natural persons would arise, and the data controller considers that it is not possible to mitigate this threat with reasonable measures from the point of view of the available technology and implementation costs, before processing personal data consult with the supervisory authority before starting operations. In more detail, we recommend that you refer to the data protection impact assessment and transparency in the general manual of the Personal Data Processor of the Data Protection Inspectorate, which is available at www.aki.ee/juhised (impact assessment is discussed in more detail in chapter 5, pre-consultation in chapter 6 and transparency in chapter 10). Remember!

- Personal data should only be processed if the purpose cannot reasonably be achieved by other means.
- The controller must make sure that the legal basis chosen by him for processing personal data is the most appropriate in a specific situation.
- Personal data must be relevant, sufficient and limited to what is unavoidably necessary for the purpose of their processing.
- Regardless of the legal basis, the controller must always comply with the general obligations set forth in Article 5 of the IKÜM, including the principles of legality, fairness, suitability for purpose, minimality, correctness, limitation of storage, proportionality, confidentiality, security and transparency.
- Legitimate interest, performance of a contract and consent can coexist as legal bases for data processing within the framework of one legal relationship, but it is always necessary to distinguish which data is processed on which legal basis.
- Relying on the basis of legitimate interest requires that the controller has taken into account all the relevant rights and interests of the data subject and carried out a weighing of interests.
- The legitimate interest must be legal, sufficiently clearly formulated, real and present (not speculative).
- Legitimate interest must be assessed periodically. Due to circumstances that have changed over time, the

legitimate interest may end or the interests of the data subject may prove to be more important. At the end of the legitimate interest, the personal data must be deleted or transferred to a non-personalized form. 12 □ The data protection conditions should clearly distinguish data processing by purpose and determine the legal bases and the composition of the processed personal data. □ In the case of special types of personal data, there is no general basis of legitimate interest. □ The public sector can only rely on a legitimate interest outside the core business. □ In case of objection by the data subject, the controller must carry out a new assessment based on the specific situation of this data subject. □ If the legitimate interest of the controller or a third party or third parties ends, the processing of personal data must not be stopped.