weizenbaum
institut

# The Concept of "Risk" in the GDPR – an Overview

Dr. Zohar Efroni, Lena Mischau, Marie Schirmbeck, Jakob Metzger

[v. 06 May 2019]

The following table of references provides a comprehensive guide to the notion of "risk" as mentioned explicitly and implicitly within the recitals and articles of the GDPR. The aim of this working document is to provide background information regarding the authors' project on privacy icons and to complement their paper titled "Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing" (forthcoming).

| Reference | Wording[1] |
|---|---|
| **Recital 28** (pseudonymisation) | The application of pseudonymisation to personal data can **reduce the risks** to the data subjects concerned and help controllers and processors to meet their data-protection obligations. […] |
| **Recital 38** (children) | Children **merit specific protection** with regard to their personal data, as they may be **less aware of the risks**, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the **purposes of marketing or creating personality or user profiles** and the collection of personal data with regard to children when using **services offered directly to a child**. […] |
| **Recital 39** (principles of lawful processing) | Any processing of personal data should be **lawful and fair**. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. **Natural persons should be made aware of risks**, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate |

[1] Emphasis added by the authors.



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing. |
| **Recital 51** (sensitive personal data) | **Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection** as the context of their processing could create **significant risks to the fundamental rights and freedoms**. Those personal data should include personal data revealing racial or ethnic origin […]. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation […]. |
| **Recital 71** (profiling) | […] In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the **profiling**, implement technical and organisational measures appropriate to ensure, in particular, that **factors which result in inaccuracies in personal data are corrected** and the **risk of errors is minimised**, **secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect**. Automated decision-making and profiling based on **special categories of personal data** should be allowed only under specific conditions. […] |
| **Recital 74** (responsibility and liability of the controller) | The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the **nature, scope, context and purposes of the processing** and the **risk to the rights and freedoms of natural persons**. |
| **Recital 75** (examples of risk in the context of personal data processing) | The **risk to the rights and freedoms of natural persons**, of **varying likelihood and severity**, may result from **personal data processing which could lead to physical, material or non-material damage**, in particular: where the processing may give rise to **discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects **might be deprived of their rights and freedoms or prevented from exercising control over their personal data**; where personal data are processed which **reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures**; where **personal aspects are evaluated**, in particular analysing or predicting aspects concerning **performance at work, economic situation, health, personal** |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | **preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles**; where personal data of **vulnerable natural persons, in particular of children**, are processed; or where processing involves a **large amount of personal data** and affects a **large number of data subjects.** |
| **Recital 76** (risk evaluation) | The **likelihood and severity** of the risk to the rights and freedoms of the data subject should be determined by reference to the **nature, scope, context and purposes of the processing**. Risk should be evaluated on the basis of an **objective assessment**, by which it is established whether data processing operations involve a **risk or a high risk**. |
| **Recital 77** (guidance) | Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the **identification of the risk** related to the processing, their assessment in terms of **origin, nature, likelihood and severity**, and the identification of best practices to **mitigate the risk**, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be **unlikely to result in a high risk** to the rights and freedoms of natural persons and indicate what **measures may be sufficient in such cases to address such risk**. |
| **Recital 78** (data protection by design/default) | The **protection of the rights and freedoms of natural persons** with regard to the processing of personal data require that appropriate **technical and organisational measures** be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the **principles of data protection by design and data protection by default**. Such measures could consist, inter alia, of **minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features**. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the **right to data protection** when developing and designing such products, services and applications and, with due regard to the **state of the art**, to make sure that controllers and processors are able to fulfil their data protection obligations. […] |
| **Recital 79** (allocation of responsibilities between controller and processor) | The **protection of the rights and freedoms of data subjects** as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, **requires a clear allocation of the responsibilities** under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. |
| **Recital 80** (representative of non-EU controller /processor) | Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union […], the controller or the processor should designate a representative, **unless** the **processing is occasional, does not include** |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | **processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons**, taking into account the **nature, context, scope and purposes of the processing** […]. |
| **Recital 81** (contract between controller and processor) | The carrying-out of processing by a processor should be governed by a contract […], setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, **taking into account** the specific tasks and responsibilities of the processor in the context of the processing to be carried out and **the risk to the rights and freedoms of the data subject**. |
| **Recital 83** (security of processing) | In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks** inherent in the processing and implement measures to **mitigate those risks**, such as encryption. Those measures should ensure an **appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected**. In **assessing data security risk**, consideration should be given to the **risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed** which may in particular **lead to physical, material or non-material damage**. |
| **Recital 84** (DPIA; consultation of supervisory authority) | In order to enhance compliance with this Regulation where processing operations are **likely to result in a high risk to the rights and freedoms of natural persons**, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the **origin, nature, particularity and severity of that risk**. […] Where a data-protection impact assessment indicates that processing operations involve a **high risk** which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing. |
| **Recital 85** (notification of a personal data breach to the supervisory authority) | A personal data breach may, if not addressed in an appropriate and timely manner, result in **physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned**. Therefore, […] the controller should notify the personal data breach to the supervisory authority […], unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is **unlikely to result in a risk** to the rights and freedoms of natural persons. […] |
| **Recital 86** (communication of a personal data breach to the data subject) | The controller should communicate to the data subject a personal data breach, […] where that personal data breach is **likely to result in a high risk** to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. […] For example, the need to mitigate an **immediate risk of damage** would call for prompt communication with data subjects whereas the need to |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | implement appropriate measures against continuing or similar personal data breaches may justify more time for communication. |
| **Recital 87** (personal data breach) | It should be ascertained whether all appropriate **technological protection and organisational measures** have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the **nature and gravity of the personal data breach** and its **consequences and adverse effects for the data subject**. […] |
| **Recital 88** (personal data breach) | In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the **circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse**. […] |
| **Recital 89** (abolition of previous general notification obligation; DPIA) | […] Such indiscriminate general notification obligations [as provided for by Directive 95/46/EC] should […] be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are **likely to result in a high risk** to the rights and freedoms of natural persons **by virtue of their nature, scope, context and purposes**. Such types of processing operations may be those which in, particular, involve using **new technologies, or are of a new kind** and where no data protection impact assessment has been carried out before by the controller […]. |
| **Recital 90** (DPIA) | In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the **particular likelihood and severity of the high risk**, taking into account the **nature, scope, context and purposes of the processing and the sources of the risk**. That impact assessment should include, in particular, the **measures, safeguards and mechanisms envisaged for mitigating that risk**, ensuring the protection of personal data and demonstrating compliance with this Regulation. |
| **Recital 91** (examples of cases where DPIA is necessary) | This should in particular apply to **large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights**. A data protection impact assessment should also be made where personal data are processed for taking **decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures**. A data protection impact assessment is equally required for **monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority** |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | **considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale**. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory. |
| **Recital 92** (cases where subject of DPIA may be broader than a single project) | There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where **public authorities or bodies intend to establish a common application or processing platform** or where **several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity**. |
| **Recital 94** (consultation of supervisory authority) | Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a **high risk** to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. **Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person**. […] |
| **Recital 96** (consultation of supervisory authority in the context of legislative /regulatory measures) | A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to **mitigate the risk** involved for the data subject. |
| **Recital 97** (data protection officer) | Where the processing is carried out by a public authority […], where, in the private sector, processing is carried out by a controller whose **core activities** consist of processing operations that require **regular and systematic monitoring of the data subjects on a large scale**, or where the core activities of the controller or the processor consist of processing **on a large scale of special categories of personal data and data relating to criminal convictions and offences**, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. […] The **necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required** for the personal data processed by the controller or the processor. |
| **Recital 98** (codes of conduct) | Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct […]. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the **risk likely to result from the processing** for the rights and freedoms of natural persons. |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| **Recital 122** (supervisory authorities' competences) | Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. […] This should include […] **promoting public awareness of the risks**, rules, safeguards and rights in relation to the processing of personal data. |
| **Art. 4 no. 24** (definitions) | […] 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the **significance of the risks** posed by the draft decision as regards the **fundamental rights and freedoms of data subjects** and, where applicable, the free flow of personal data within the Union; |
| **Art. 23(2)(g)** (restrictions) | In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:<br>(g) the **risks to the rights and freedoms of data subjects** […] |
| **Art. 24(1)** (responsibility of the controller) | Taking into account the **nature, scope, context and purposes of processing** as well as the **risks of varying likelihood and severity for the rights and freedoms of natural persons**, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. |
| **Art. 25(1)** (data protection by design / default) | Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the **risks of varying likelihood and severity for rights and freedoms of natural persons** posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate **technical and organisational measures**, such as pseudonymisation, which are **designed to implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. |
| **Art. 25(2)** (data protection by design/default) | The controller shall implement appropriate **technical and organisational measures** for ensuring that, by default, **only personal data which are necessary** for each specific purpose of the processing are processed. That obligation applies to the **amount** of personal data collected, the **extent** of their processing, the **period of their storage** and their **accessibility**. In particular, such measures shall ensure that by default personal data are **not made accessible without the individual's intervention to an indefinite number of natural persons**. |
| **Art. 27(2)(a)** (representative of non-EU controller /processor) | [The obligation to designate a representative in the EU shall not apply to:] processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is **unlikely to result in a risk to the rights and freedoms of natural persons**, taking into account the nature, context, scope and purposes of the processing […] |
| **Art. 30(5)** (records of processing activities) | The obligations [to maintain a record of (all categories of) processing activities] shall not apply to an enterprise […] employing fewer than 250 persons unless the processing it carries out is **likely to result in a risk to the rights and freedoms of** |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | **data subjects**, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10. |
| **Art. 32(1)(a)-(d)** (security of processing) | Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the **risk of varying likelihood and severity for the rights and freedoms of natural persons**, the controller and the processor shall implement appropriate **technical and organisational measures** to **ensure a level of security appropriate to the risk**, including inter alia as appropriate:<br>(a) the pseudonymisation and encryption of personal data;<br>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;<br>(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;<br>(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. |
| **Art. 32(2)** (security of processing) | In assessing the appropriate level of security account shall be taken in particular of the **risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed**. |
| **Art. 33** (notification of a personal data breach to the supervisory authority) | (1) In the case of a personal data breach, the controller shall […] notify the personal data breach to the supervisory authority […], unless the personal data breach is **unlikely to result in a risk to the rights and freedoms of natural persons**. […]<br>(3) The notification […] shall at least:<br>(a) describe the **nature** of the personal data breach including where possible, the **categories and approximate number of data subjects** concerned and the **categories and approximate number of personal data records** concerned;<br>(b) […]<br>(c) describe the **likely consequences** of the personal data breach;<br>(d) describe the **measures** taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to **mitigate its possible adverse effects**.<br>(4) (..)<br>(5) The controller shall document any personal data breaches, comprising the **facts** relating to the personal data breach, its **effects** and the **remedial action** taken. […] |
| **Art. 34** (communication of a personal data breach to the data subject) | (1) When the personal data breach is **likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall communicate the personal data breach to the data subject without undue delay.<br>(2) The communication to the data subject […] shall describe in clear and plain language the **nature** of the personal data breach and contain at least the **information and measures referred to in points (b), (c) and (d) of Article 33(3)**.<br>(3) The communication to the data subject […] shall not be required if any of the following conditions are met:<br>(a) the controller has implemented appropriate **technical and organisational protection measures**, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | (b) the controller has taken **subsequent measures** which ensure that the **high risk to the rights and freedoms of data subjects** referred to in paragraph 1 **is no longer likely to materialise**;<br>(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure […].<br>(4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the **likelihood of the personal data breach resulting in a high risk**, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met. |
| **Art. 35**<br>(DPIA) | (1) Where a type of processing in particular using **new technologies**, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A **single assessment may address a set of similar processing operations that present similar high risks**.<br>(2) […]<br>(3) A data protection impact assessment […] shall in particular be required in the case of:<br>(a) a **systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect** the natural person;<br>(b) processing **on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10**; or<br>(c) a **systematic monitoring of a publicly accessible area on a large scale**.<br>(4) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment […].<br>(5) The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. […]<br>(6) […]<br>(7) The assessment shall contain at least:<br>(a) a systematic **description of the envisaged processing operations and the purposes** of the processing, including, where applicable, the legitimate interest pursued by the controller;<br>(b) an assessment of the **necessity and proportionality** of the processing operations in relation to the purposes;<br>(c) an assessment of the **risks to the rights and freedoms of data subjects** referred to in paragraph 1; and<br>(d) the **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.<br>(8) Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account […].<br>(9) […]<br>(10) Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de

| | |
|---|---|
| | law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary […].<br>(11) Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a **change of the risk** represented by processing operations. |
| **Art. 36(1)** (consultation of supervisory authority) | The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the **processing would result in a high risk** in the absence of measures taken by the controller to mitigate the risk. |
| **Art. 39(2)** (data protection officer) | The data protection officer shall in the performance of his or her tasks have due regard to the **risk associated with processing operations**, taking into account the nature, scope, context and purposes of processing. |
| **Art. 49(1)(a)** (transfers of personal data to third countries /international organisations) | In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46 […], a transfer […] of personal data to a third country or an international organisation shall take place only on one of the following conditions:<br>(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the **possible risks of such transfers for the data subject** due to the absence of an adequacy decision and appropriate safeguards; |
| **Art. 57(1)(b), (k)** (supervisory authority) | (1) […] each supervisory authority shall […]<br>(b) **promote public awareness and understanding of the risks**, rules, safeguards and rights in relation to processing. […]<br>(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4) |
| **Art. 70(1) s. 2 (h)** (EDPB) | [T]he board shall […] issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is **likely to result in a high risk to the rights and freedoms of the natural persons** referred to in Article 34(1). |



Weizenbaum-Institut, Hardenbergstr. 32, 10623 Berlin
www.weizenbaum-institut.de