Privacy Policy

This privacy notice (hereinafter referred to as the "Notice") aims to inform you, as a visitor of the website www.ilonacallsluxury.com (hereinafter referred to as the "Website"), about how your personal data is handled during the operation of the Website and your visits made through it.

I reserve the right to amend this Notice, of which I will duly inform the data subjects. Information related to data processing will be published on the website www.ilonacallsluxury.com.

My objective is to inform you in a concise, transparent, intelligible and easily accessible manner—clearly and in plain language—about the rights you hold in relation to the processing of your personal data and how you can exercise these rights.

The data controller of the Website (hereinafter referred to as the "Controller") is Ilona Orbók (website: www.ilonacallsluxury.com, e-mail address: info@ilonacallsluxury.com). Since Article 37 of the GDPR does not make it mandatory in our case, no data protection officer has been appointed.

Regarding the scope of data processed by the Controller, it is important to inform you that I only request the provision of personal data from the visitors of my website if they complete the contact form. I do not link the personal data provided in connection with using the contact form, and identifying my visitors is fundamentally not my intention.

You provide your personal data voluntarily via the contact form and during communication with me; therefore, I kindly ask you to pay particular attention to the truthfulness, correctness, and accuracy of the data you provide, as you are responsible for them.

If you provide personal data not of yourself but of another person, I presume that you are authorised to do so.

The personal data of a person under the age of 16 may only be processed with the consent of an adult who exercises parental responsibility over them. Neither the Controller nor I are able to verify the authorisation of the person providing such consent or the content of their declaration; therefore, it is the User and the person exercising parental responsibility who guarantee that the consent complies with the applicable legislation.

You may withdraw your consent to the processing of your personal data at any time, free of charge,

- by withdrawing your consent to data processing, or
- by withdrawing your consent to the processing or use of any data that is required to be provided during the contact process, or by requesting that such data be blocked.

I undertake to register the withdrawal of consent within a period of 30 days due to technical reasons. However, please note that for the purpose of fulfilling my legal obligations or asserting my legitimate interests, I may continue to process certain data even after the withdrawal of your consent.

In the case of the use of misleading personal data, or if any of my visitors commit a criminal offence or attack the system of my website, I will immediately delete their data upon termination of their registration or, where necessary, retain the data for the duration of establishing civil liability or conducting criminal proceedings.

Your data may only be transferred within the scope and under the conditions specified by law.

The court, the public prosecutor's office, and other authorities (e.g. the police, the tax authority, or the National Authority for Data Protection and Freedom of Information) may request information, the disclosure of data or documents. In such cases, I am obliged to comply with the request for data provision, but only to the extent that is strictly necessary for the purpose of the request.

The contributors and employees involved in the Controller's data management and/or data processing are entitled to access your personal data to a pre-determined extent and are bound by a confidentiality obligation.

Your personal data is protected by appropriate technical and other measures. I ensure the security and availability of your data, and safeguard it against unauthorised access, alteration, damage, disclosure or any other unauthorised use.

As part of organisational measures, physical access to the Controller's premises is monitored, employees receive continuous training, and paper-based documents are stored securely. As part of technical measures, encryption, password protection and antivirus software are used. However, please note that data transmission over the Internet cannot be regarded as fully secure. While the Controller takes every possible step to ensure the highest level of security in its processes, I cannot assume full responsibility for data transmission via my website. However, strict regulations are observed regarding any data received by me or the Controller, to protect your data and prevent unauthorised access.

I protect your personal data with appropriate technical and other measures, and I ensure the security and availability of the data, as well as safeguard it against unauthorised access, alteration, damage, disclosure, or any other unauthorised use.

As part of organisational measures, physical access is controlled at the Controller's premises, employees receive continuous training, and paper-based documents are stored with appropriate protection. As part of technical measures, encryption, password protection, and antivirus software are used.

However, I would like to draw your attention to the fact that data transmission over the Internet cannot be considered completely secure. The Controller takes all possible steps to make the processes as secure as possible, but I cannot take full responsibility for data transmission via my website. Nevertheless, we apply strict regulations with respect to the data received by me or by the Controller to ensure the security of your data and prevent unlawful access.

During data processing, so-called cookies (hereinafter: "cookies") are placed on my website for the purpose of providing customised services. The aim of cookies is to ensure the highest possible level of operation of the site, to provide personalised services, and to enhance the user experience. Cookies are small data files that are placed on your computer using the website and are saved and stored by your internet browser.

Most used internet browsers (e.g. Chrome, Firefox, etc.) accept and allow the download and use of cookies by default. However, it is up to you to modify your browser settings to reject or disable cookies, and you can also delete previously stored cookies from your computer. More detailed information about the use of cookies can be found in the "Help" section of your browser.

Some cookies do not require your prior consent. My website provides brief information about these at the beginning of your first visit. Such cookies include session cookies that assist with authentication, multimedia playback, load balancing, user interface customisation, and user-centric security cookies.

For cookies that require consent—if data processing begins upon visiting the site—you will be informed at the start of your first visit and your consent will be requested.

My website does not use or permit the use of cookies that allow third parties to collect data without your consent. Accepting cookies is not mandatory, but the Controller accepts no liability if, due to the lack of cookie authorisation, the website does not function as expected.

The cookies used by my website are as follows:

Name	**_ga**	**_gat**	**_gid**
Provider	orbokilona.hu	orbokilona.hu	orbokilona.hu
Purpose	Registers a unique identifier that generates statistical data on how the visitor uses the website.	Stores the throttle request rate used by Google Analytics.	Registers a unique identifier that generates statistical data on how the visitor uses the website.
Expiry	2 years	Session	Session
Type	HTTP	HTTP	HTTP

You can read more about third-party cookies on this page.

If you have any questions regarding data processing, you may request further information by writing to info@ilonacallsluxury.com. I will respond to your query within 15 days (but no later than one month) to the contact details you have provided.

During data processing, you have the following rights and legal remedies:

You may:

- **request information** about the processing of your data,
- **request the rectification, modification, or supplementation** of the personal data I process about you,
- **object to data processing** and request the **erasure or restriction** of your data (except in cases of mandatory processing),
- **seek remedy before a court**,
- **lodge a complaint with the supervisory authority** or initiate a procedure (https://naih.hu/panaszuegyintezes-rendje.html).

Supervisory Authority: National Authority for Data Protection and Freedom of Information (Address: H-1055 Budapest, Falk Miksa utca 9-11., Mailing address: H-1363 Budapest, P.O. Box: 9, Telephone: +36 (1) 391-1400, Fax: +36 (1) 391-1410, Email: ugyfelszolgalat@naih.hu, Website: https://naih.hu)

At your request, I will provide information on:

- the **data** I process or have processed about you,
- their **source**,
- the **purpose and legal basis** of the data processing,
- the **duration** of the processing or, if that is not possible, the criteria for determining that duration,

- the **name and address of my data processors** and their activities related to data processing,
- the **circumstances and effects of any data protection incidents** and the measures taken to prevent or mitigate them,
- and, in the case of **data transfers**, the legal basis and the recipient of the transfer.

I will provide this information within 15 days (but no later than one month) from the submission of your request. The information is free of charge unless you have already submitted a request regarding the same data set within the current year. Any fee you may have already paid will be refunded if the data were processed unlawfully or if the request for information results in rectification. I may only refuse to provide information in cases defined by law, citing the legal basis, and informing you of your right to seek remedy in court or with the Authority.

You and all those to whom I have previously transferred the data for processing purposes will be notified of any **rectification, restriction, marking, or erasure** of personal data, unless such notification would violate your legitimate interest.

If I do not comply with your request for rectification, restriction or erasure, I will notify you in writing (or electronically with your consent) within 15 days (but no later than one month) of receiving the request, stating the reasons for the refusal and informing you of your right to seek judicial remedy and to turn to the Authority.

If you object to the processing of your personal data, I will examine your objection within 15 days (but no later than one month) from the receipt of the request and notify you in writing of my decision. If your objection is deemed valid, I will terminate the data processing – including further data collection and transmission – and block the data. I will also notify everyone to whom I previously transferred the data affected by the objection and who must take steps to enforce the right to object.

I may refuse to comply with your request if I can demonstrate that the processing is justified by compelling legitimate grounds which override your interests, rights and freedoms, or which relate to the establishment, exercise or defence of legal claims. If you do not agree with my decision, or if I fail to respond within the specified timeframe, you may bring the matter before a court within 30 days from the date the decision was communicated or from the last day of the deadline.

Data protection litigation falls under the jurisdiction of the regional court. The case may – at the data subject's discretion – also be brought before the regional court having jurisdiction over their residence or place of stay. Foreign nationals may also submit complaints to the supervisory authority in their country of residence.

I kindly ask you to contact me first before turning to the supervisory authority or the court, to attempt to resolve the issue as quickly and effectively as possible through consultation.

During data processing, I pay particular attention to adhering to the following data protection and data management principles, and I acknowledge and undertake to follow the data protection and data management policy as binding upon me.

- I process personal data lawfully, fairly and in a manner that is transparent to you.
- I collect personal data only for specified, explicit and legitimate purposes, and do not process them in a manner that is incompatible with those purposes.
- The personal data I collect, and process are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- I take all reasonable steps to ensure that the personal data I process are accurate and, where necessary, kept up to date; inaccurate personal data will be erased or rectified without delay.
- I store personal data in a form which permits your identification only for as long as is necessary for the purposes of the processing.
- I ensure the appropriate security of personal data through appropriate technical and organisational measures, protecting them against unauthorised or unlawful processing, accidental loss, destruction or damage.

Your personal data are processed by me:

- based on your prior informed and voluntary consent, solely to the extent necessary, and always for a specific purpose — that is, I collect, record, organise, store and use such data only in this context.
- in certain cases, based on legal obligations, in which case I shall expressly draw your attention to this fact.
- in certain cases, based on the legitimate interest of the Data Controller or a third party, such as for the operation, development and security of our website.

Throughout the data processing activity, I ensure that the management, storage and transmission of personal data comply with and are in accordance with the applicable laws and regulations (in particular the following), as well as the guidelines of the Article 29 Working Party under the Data Protection Directive, and the data protection practices established by the National Authority for Data Protection and Freedom of Information (hereinafter: the "Authority"):

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data (General Data Protection Regulation – GDPR);
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Info Act);
- Act V of 2013 on the Civil Code (Ptk.);
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (E-Commerce Act);
- Act C of 2003 on Electronic Communications (ECA);

- Act CLV of 1997 on Consumer Protection (CPA);
- Act CLXV of 2013 on Complaints and Public Interest Disclosures.
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities.

Data Protection Glossary

- **Data protection**: the set of principles, rules, procedures, data processing tools and methods that ensure the lawful handling of personal data and the protection of the data subjects.
- **Personal data**: any information relating to an identified or identifiable natural person (data subject); and any conclusion that can be drawn about the data subject from such data.
- Personal data shall retain its status as personal data during processing if the link to the data subject can be restored. The link to the data subject can be restored if the Data Controller possesses the technical means necessary for such restoration.
- **Data subject**: any natural person who is identified or identifiable, directly or indirectly, based on specific personal data. A person is considered identifiable if he or she can be identified – directly or indirectly – by reference to a name, an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
- **Special category data**: personal data revealing racial or ethnic origin, political opinions or party affiliation, religious or philosophical beliefs, trade union membership, sexual life, health status, addiction, or criminal personal data.
- **Criminal personal data**: personal data generated in connection with criminal proceedings or prior to them, concerning criminal offences or criminal proceedings, held by authorities authorised to conduct such proceedings or detect crimes, or by the penal enforcement agency, and data concerning criminal records.
- **Data processing**: any operation or set of operations performed on data, regardless of the method used, such as collection, recording, organisation, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, restriction, deletion or destruction, as well as prevention of further use, and the capturing of photo, audio or video recordings, and recording of physical characteristics suitable for identifying a person (e.g., fingerprints, palm prints, DNA samples, iris scans).
- **Data controller**: the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data, makes and implements decisions concerning data processing (including the tools used), or has such processing carried out by a processor acting on its behalf.
- **Data processing (technical)**: the performance of technical tasks related to the data processing operations (regardless of the method or device used for executing the operations or the location of application).

- **Data processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller, under a contract concluded with the data controller — including contracts entered under statutory provisions.
- **Rights of the data subject**: the data subject must be informed of all details of the data processing prior to the commencement of processing, and upon request at any time. The data subject has the right to request the rectification or, in certain cases, deletion of their data, and may object to the processing of their personal data in cases specified by law.
- **Legal basis of data processing**: as a rule, the data subject's consent or mandatory data processing prescribed by law.
- **Consent:** the data subject's voluntary and explicit declaration of will, based on adequate information, by which they unambiguously agree to the processing of their personal data — either fully or for specific operations. In the case of special categories of data, written form is required.
- **Adequate information:** prior to the commencement of data processing, the data subject must be informed whether the processing is based on their consent or is mandatory, and must be clearly and comprehensively informed about all facts relating to the processing of their data, particularly the purpose and legal basis of data processing, the identity of the person authorized to process and handle the data, the duration of the data processing, and the persons entitled to access the data. The information must also cover the data subject's rights related to data processing and the available remedies.
- **Objection:** the declaration by the data subject by which they object to the processing of their personal data and request the termination of the processing and deletion of the processed data.
- **Data security:** a system of technical and organizational measures to prevent unauthorized acquisition, alteration, or destruction of data.
- **Principles of data processing:** the requirement of purpose limitation (see below) and the requirement of data quality. The latter includes the necessity for accurate, complete, and up-to-date data, as well as the fairness and lawfulness of data collection and processing.
- **Purpose limitation in data processing:** personal data may only be processed for a specified purpose, in the exercise of legal rights and performance of obligations. Data processing at every stage must comply with the purpose of data processing; the collection and processing of data must be fair and lawful. Only personal data essential to achieving the purpose of data processing and suitable for achieving that purpose may be processed. Personal data shall be processed only to the extent and for the duration necessary for the realization of the purpose. Data processing must ensure that data are accurate, complete, and, if necessary for the purpose of processing, up to date, and that the data subject can be identified only for the duration necessary for the purpose of data processing.
- **Transfer of data abroad:** the transfer of personal data to a data controller conducting data processing activities in a third country outside the EEA (European Economic Area: the member states of the European Union, as well as Iceland, Norway, and Liechtenstein).
- **Freedom of information:** the fundamental right to access and disseminate data of public interest and data that are public for public interest reasons, which facilitates societal control over the exercise of public authority and transparency in the operation of public institutions and the spending of public funds.
- **Data of public interest:** any information or knowledge recorded in any form or manner, independent of its mode of processing or whether it is an individual or collective piece of data, held by an authority performing state/municipal or other public duties, related to its activities or generated in connection with fulfilling its public duties, excluding personal data (including, but not limited to, data concerning jurisdiction, competence, organizational

structure, professional activities, their effectiveness, data types held, regulations governing operations, economic management, and concluded contracts).

- **Public data for reasons of public interest:** all data not falling under the definition of data of public interest, the disclosure, accessibility, or availability of which is mandated by law for reasons of public interest. (For example, laws on real estate registry, company law, and accounting classify a wide range of data as public for reasons of public interest in order to protect creditor interests and ensure market security.)
- **Avtv.**: Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest, the first data protection law after the regime change, which was in force until 31 December 2011. It was repealed as of 1 January 2012 by the Infotv. (see below).
- **Infotv.**: Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information, adopted by the National Assembly pursuant to Article VI of the Fundamental Law, to ensure the right to informational self-determination and freedom of information, establishing the fundamental rules serving the enforcement of these rights and the supervisory authority (NAIH). The purpose of the Act is to ensure respect for the private sphere of natural persons by data controllers and to realize the transparency of public affairs through the right to access and disseminate data of public interest and data public for reasons of public interest. It has been in force since 1 January 2012.
- **NAIH**: National Authority for Data Protection and Freedom of Information: the national data protection authority established by the Infotv. on 1 January 2012, replacing the institution of the Data Protection Commissioner, responsible for protecting the two informational rights and supervising the legality of data processing in Hungary.
- **EDPS (European Data Protection Supervisor)**: Established in 2004, the European Data Protection Supervisor is an independent institution supervising the processing of personal data by European institutions and bodies. It also plays a key role in the development of European data protection case law and interpretation.
- **Internal Data Protection Officer:** the employee within the data controller/data processor's organization who reports directly to the head of the organization and is responsible on behalf of the organization for compliance with data protection rules and the protection of personal data.
- **Council of Europe Data Protection Convention:** The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, concluded in Strasbourg on 28 January 1981 (the Council of Europe Convention No. 108). It is the first significant binding international legal document in the field of data protection for the signatory states. It was promulgated in Hungary by Act VI of 1998 on 27 February 1998.
- **EU Data Protection Directive:** Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This general data protection directive of the European Union, adopted on 24 October 1995, among others, established the so-called Article 29 Working Party (see below).
- **Article 29 Working Party:** An independent advisory, consultative, and opinion-forming body composed of the data protection commissioners or authorities of the Member States as defined in Article 29 of Directive 95/46/EC. Through its opinions and recommendations, it assists the European Commission in protecting the informational self-determination rights of European citizens.
- **EU Data Protection Regulation Proposal (the "Proposed Regulation"):** The legislative package prepared for 2012 includes both the draft General Data Protection Regulation (see below) and the draft directive regulating police and criminal justice data processing.
- **EU Data Protection Regulation Proposal:** The proposal published by the European Commission on 25 January 2012 aiming at a comprehensive reform of European data

protection rules and the establishment of a more uniform, simpler, and modern regulation at EU level for the processing of personal data of European citizens. Unlike a directive, the regulation as a legal source is directly applicable in EU Member States, guaranteeing immediate and unconditional legal harmonization at EU level. The proposal is first discussed by the Member States and the European Parliament, and if adopted by the European Parliament, two years are required for it to enter into force.

- **Schengen/SIS:** The creation of the Schengen Area is the most important EU achievement enabling the free movement of persons. The security risks arising from the abolition of internal borders and the tightened control of external borders are managed by the Schengen Information System (SIS), Europe's largest IT system, primarily through effective data sharing. Member States enter alerts into the SIS related to wanted or missing persons, stolen or lost property, and entry bans. Data subjects may submit data protection requests related to SIS (such as requests for information or rectification) to any police station or Hungarian diplomatic mission, which forwards them to the ORFK NEBEK SIRENE Office. The lawfulness of Hungarian SIS data processing is supervised by the NAIH.
- **EURODAC:** (European Dactyloscopy) The European fingerprint database established by Regulation 2725/2000/EC, primarily aimed at identifying asylum seekers and illegal migrants.
- **OECD Guidelines:** Guidelines on the protection of privacy and transborder flows of personal data adopted by the Council of the Organisation for Economic Co-operation and Development (OECD), which came into effect on 23 September 1980.
- **BCR (Binding Corporate Rules):** Mandatory codes of conduct approved by the data protection authority of the EU Member State where the multinational company is registered. Under these rules, the multinational group commits to ensuring that personal data transferred within the group from EU Member States to third countries outside the EU benefit from a level of protection that exceeds the usual protection standards in the destination country.
- **ACTA (Anti-Counterfeiting Trade Agreement):** An international agreement aimed at enabling authorities to combat piracy and counterfeit goods distributed online. Officially proposed by Japan, the agreement was opened for signature in March 2011. During international negotiations, the European Data Protection Supervisor (EDPS) expressed concerns in February 2010 about the compatibility of the agreement with EU data protection rules. The European Union did not accede to the agreement.
- **BAR-list:** The former name of the Hungarian Central Credit Information System (KHR). The KHR consists of two subsystems for retail banking customers. The negative list subsystem contains data on debtors with delayed payments or credit defaults, while the positive list subsystem includes all client and contract data submitted by credit institutions concerning all Hungarian borrowers. Credit history data from the positive list may only be accessed by banks with the explicit consent of the loan applicant to better assess creditworthiness.
- **CCTV (Closed-Circuit Television):** A closed-circuit television surveillance system consisting of multiple cameras designed for constant security monitoring of a designated area. Unlike publicly broadcast "open circuit" television, CCTV footage is accessible only to a closed group (typically security personnel). The widespread use of CCTV systems has sparked debates about possible negative impacts on personal rights and data protection.
- **PNR (Passenger Name Records):** The airline passenger record data set primarily consists of data provided by the passenger during booking and data collected by the airline related to the travel. These data are stored by airlines and airport control centers, but in certain cases, law enforcement authorities may gain access. EU regulation of PNR data processing is ongoing, as some data protection issues require special consideration. The

previously highly debated agreement between the EU and the United States on airline passenger data exchange entered into force on July 1, 2012.

- **Cloud Computing:** A broad term encompassing numerous IT services provided not by the user's own computer or corporate data center, but by remote servers located anywhere in the world. Common cloud services include internet mail systems, storage services, development environments, and virtual workstations. Examples include Gmail and Dropbox. Cloud computing allows clients to access IT systems cost-effectively and flexibly without heavy investments or dedicated staff. However, cloud computing raises many data protection concerns: user-uploaded data constantly moves between locations without the user's knowledge; providers may use personal data for their own purposes (often marketing); subcontractors worldwide may process data without the client's awareness; and complex corporate applications may make data extraction difficult and costly, complicating switching providers.
- **Cookies:** Small data files placed on a user's computer by a visited website, aimed at facilitating and improving the internet service experience. Cookies fall generally into two categories: temporary cookies, used during a session (e.g., security verification during online banking), and persistent cookies (e.g., site language preferences), which remain until deleted by the user. According to European Commission guidelines, cookies [except those strictly necessary for the service] may only be placed with the user's consent. Cookies raise data protection issues, notably because they enable tracking of browsing habits.
- **Privacy by Default:** A data protection approach where the collection, processing, or handling of personal data occurs solely upon the explicit request of the data subject. Data controllers' fundamental "default" position must be to always consider data protection aspects and act accordingly in data processing activities.
- **Privacy by Design:** Originating in Canada in the 1990s, this data protection approach emphasizes that compliance with legal regulations alone is insufficient. Organizations must embed data protection principles into their operations as a fundamental organizational principle. Data protection considerations are incorporated from the design phase of operational processes, ensuring full enforcement of data protection. This approach is closely related to the "privacy by default" concept.

Adatvédelmi Tájékoztató

Jelen **adatkezelési tájékoztató** (a továbbiakban: „Tájékoztató") célja, hogy Ön, mint www.ilonacallsluxury.com honlap (a továbbiakban: Weboldal) látogatója megismerje, hogy a weboldal működtetése, valamint a weboldalon keresztül történő látogatás sorűn a személyes adatait milyen módon kezelem.

Jelen Tájékoztató módosítására fenntartom a jogot, amelyről az érintetteket megfelelő módon tájékoztatom. Az adatkezeléssel kapcsolatos információk közzététele a www.ilonacallsluxury.com weboldalon történik.

Célom, hogy tömör, érthető és könnyen hozzáférhető formában, átláthatóan, világosan és közérthetően megfogalmazva tájékoztassam Önt arról, hogy személyes adatainak kezelése kapcsán milyen jogokkal rendelkezik, illetve ezen jogait milyen módon tudja érvényesíteni

A weboldalam adatkezelője (a továbbiakban: Adatkezelő) a Orbók Ilona (weboldal: www.ilonacallsluxury.com , e-mail cím: info@ilonacallsluxury.com). Tekintettel arra, hogy a GDPR. 37. cikke esetünkben nem teszi kötelezővé, adatvédelmi tisztviselő nem került kinevezésre.

Az **Adatkezelő által kezelt adatok köre** vonatkozásában fontos tájékoztatnom Önt, hogy a weboldalam látogatóit csak akkor kérem **személyes adatainak megadására, ha a kapcsolatfelvételi űrlapot kitöltik**. A kapcsolatfelvétel igénybevétele kapcsán megadott személyes adatokat nem kapcsolom össze és a látogatóim beazonosítása alapvetően nem célom.

A **személyes adatokat** Ön önkéntesen bocsátja rendelkezésem a Kapcsolatfelvételi űrlapon, illetve a velem történő kapcsolattartása során, éppen ezért kérem, hogy adatai közlésekor fokozatosan ügyeljen azok valódiságára, helyességére és pontosságára, mert ezekért Ön felelős.

Amennyiben Ön nem a saját, hanem más személy személyes adatait adja meg, úgy vélelmezem, hogy Ön az ehhez szükséges felhatalmazással rendelkezik.

A 16. életévét be nem töltött személy érintett személyes adatait csak a felette szülői felügyeletet gyakorló nagykorú személy hozzájárulása esetén kezelhető. Az Adatkezelőnek, illetve nekem nem áll módomban a hozzájáruló személy jogosultságát, illetve nyilatkozatának tartalmát ellenőrizni, így a Felhasználó, illetve a felette szülői felügyeletet gyakorló személy szavatol azért, hogy a hozzájárulás megfelel a jogszabályoknak.

Ön az **adatkezeléshez adott hozzájárulás**át bármikor ingyenesen visszavonhatja

- az adatkezeléshez hozzájárulás visszavonásával, illetve
- a kapcsolatfelvétel során feltétlen kitöltendő bármely adat kezeléséhez vagy felhasználásához való hozzájárulás visszavonásával vagy zárolásának kérésével.

A **hozzájárulás visszavonásának regisztrálását** – technikai okokból 30 napos határidővel vállalom, azonban felhívom a szíves figyelmét arra, hogy jogi kötelezettségem teljesítése vagy jogos érdekeim érvényesítése céljából bizonyos adatokat a hozzájárulás visszavonása után is kezelhetek.

Megtévesztő személyes adat használata esetén, illetve, ha valamelyik látogatóm bűncselekményt követ el vagy weboldalam rendszerét támadja, az adott látogató regisztrációjának megszüntetésével egyidejűleg adatait haladéktalanul törlöm, illetve – szükség esetén – megőrzöm azokat a polgári jogi felelősség megállapításának vagy büntető eljárás lefolytatásának időtartama alatt.

Az Ön adatait csak jogszabályban meghatározott keretek között és feltételek mellett **továbbíthatom**.

A bíróság, az ügyészség és más hatóságok (pl. rendőrség, adóhivatal, Nemzeti Adatvédelmi és Információszabadság Hatóság) tájékoztatás adása, adatok közlése vagy iratok rendelkezésre bocsátása miatt megkereshetnek. Ezekben az esetekben adatszolgáltatási kötelezettségemet teljesítenem kell, de csak a megkeresés céljának megvalósításához elengedhetetlenül szükséges mértékben.

Az Adatkezelő adatkezelésében és/vagy adatfeldolgozásában részt vevő közreműködői és munkavállalói előre meghatározott mértékben – titoktartási kötelezettség terhe mellett – jogosultak az Ön személyes adatait megismerni.

Az Ön **személyes adat**ait megfelelő technikai és egyéb intézkedésekkel **védem**, valamint **biztosítom az adatok biztonságát, rendelkezésre állását, továbbá óvom azokat a**

jogosulatlan hozzáféréstől, megváltoztatástól, sérülésektől, illetve nyilvánosságra hozataltól és bármilyen egyéb jogosulatlan felhasználástól.

Szervezeti intézkedések keretében az Adatkezelő épületeiben ellenőrzik a fizikai hozzáférést, munkavállalóikat folyamatosan oktatják és a papír alapú dokumentumokat megfelelő védelemmel elzárva tartják. A technikai intézkedések keretében titkosítást, jelszóvédelmet és vírusirtó szoftvereket használnak. Felhívom azonban a szíves figyelmét arra, hogy az interneten keresztüli adattovábbítás nem tekinthető teljeskörűen biztonságos adattovábbításnak. Az Adatkezelő mindent megtesz annak érdekében, hogy a folyamatokat minél biztonságosabbá tegye, a weblapomon keresztül történő adattovábbításért azonban nem tudok teljes felelősséget vállalni, ám a hozzám, illetve az Adatkezelőhöz beérkezett adatok tekintetében szigorú előírásokat tartunk be az Ön adatainak biztonsága és a jogellenes hozzáférés megakadályozása érdekében.

Az **adatkezelés során** a testre szabott szolgáltatás érdekében **a weboldalamon úgynevezett ún. cookie-k** (a továbbiakban: **sütik**) **kerültek elhelyezésre**. A sütik célja az adott oldal minél magasabb színvonalú működésének biztosítása, személyre szabott szolgáltatások biztosítása, a felhasználói élmény növelése. A sütik olyan kisméretű adatfájlok, amelyek a weboldalon keresztül a weboldal használatával kerülnek az Ön számítógépére úgy, hogy azokat az Ön internetes böngészője menti le és tárolja el. A leggyakrabban használt internetes böngészők (Chrome, Firefox, stb.) többsége alapbeállításként elfogadja és engedélyezi a sütik letöltését és használatát, az viszont már Öntől függ, hogy a böngésző beállításainak módosításával ezeket visszautasítja vagy letiltja, illetve Ön a már a számítógépen lévő eltárolt sütiket is tudja törölni. A sütik használatáról az egyes böngészők „súgó" menüpontja nyújt bővebb tájékoztatást.

Egyes sütik nem igénylik az Ön előzetes hozzájárulását. Ezekről weboldalam az Ön első látogatásának megkezdésekor ad rövid tájékoztatást, ilyenek például a hitelesítési, multimédia-lejátszó, terheléskiegyenlítő, a felhasználói felület testre szabását segítő munkamenet-sütik, valamint a felhasználó-központú biztonsági sütik.

A hozzájárulást igénylő sütikről – amennyiben az adatkezelés már az oldal felkeresésével megkezdődik –az első látogatás megkezdésekor tájékoztatom Önt és kérem az Ön hozzájárulását.

Weboldalam nem alkalmaz és nem is engedélyez olyan sütiket, amelyek segítségével harmadik személyek az Ön hozzájárulása nélkül adatot gyűjthetnek. A sütik elfogadása nem kötelező, az Adatkezelő azonban nem vállal azért felelősséget, ha sütik engedélyezése hiányában a weblapom esetleg nem az elvárt módon működik.

A weboldalam által alkalmazott sütik a következők:

Név:	_ga	_gat	_gid
Szolgáltató:	orbokilona.hu		
Cél:	Regisztrálja az egyedi azonosítót, amely statisztikai adatokat generál arra nézve, hogy a látogató hogyan használja a webhelyet	A Google Analytics által használt thottle request szerinti arányt tárolja.	Regisztrálja az egyedi azonosítót, amely statisztikai adatokat generál arra nézve, hogy a látogató hogyan használja a webhelyet.
Lejárat:	2 év	Munkamenet	Munkamenet
Típus:	HTTP		

A harmadik féltől származó sütiről (third party cookie) részletesen ezen az oldalon olvashat.

Az adatkezeléssel kapcsolatos kérdéseivel Ön az info@ilonacallsluxury.com e-mail címen kérhet további tájékoztatást, válaszomat 15 napon belül (legfeljebb azonban 1 hónapon belül) megküldöm Önnek az Ön által megadott elérhetőségre.

Az adatkezelés során Önt az alábbi **jogok** illetik meg, illetve az alábbi **jogorvoslati lehetőségek**kel élhet.

Ön az adatkezelésről

- tájékoztatást kérhet,
- kérheti az általam kezelt személyes adatai helyesbítését, módosítását, kiegészítését,
- tiltakozhat az adatkezelés ellen és kérheti adatai törlését, valamint zárolását (a kötelező adatkezelés kivételével),
- bíróság előtt jogorvoslattal élhet,
- a felügyelő hatóságnál panaszt tehet, illetve eljárást kezdeményezhet (https://naih.hu/panaszuegyintezes-rendje.html).

Felügyelő Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (székhely: 1055 Budapest, Falk Miksa utca 9-11., postacím: 1363 Budapest, Pf.: 9, telefon: +36 (1) 391-1400, fax: +36 (1) 391-1410, e-mail: ugyfelszolgalat@naih.hu, honlap: https://naih.hu/)

Az Ön **kérelmére tájékoztatást adok** az Ön általam kezelt, illetve az általam feldolgozott

- adatairól,
- azok forrásáról,
- az adatkezelés céljáról és jogalapjáról,
- időtartamáról, ha pedig ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- az adatfeldolgozóim nevéről, címéről és az adatkezeléssel összefüggő tevékenységükről,
- adatvédelmi incidensek körülményeiről, hatásairól és az elhárításukra valamint megelőzésükre tett intézkedéseimről, továbbá
- az Ön személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről.

A kérelem benyújtásától számított 15 napon belül (legfeljebb azonban 1 hónapon belül) adom meg tájékoztatásomat. A tájékoztatás ingyenes kivéve akkor, ha Ön a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet már nyújtott be hozzám. Az Ön által már megfizetett költségtérítést visszatérítem abban az esetben, ha az adatokat jogellenesen kezeltem vagy a tájékoztatás kérése helyesbítéshez vezetett. A tájékoztatást csak törvényben foglalt esetekben tagadhatom meg jogszabályi hely megjelölésével, valamint a bírósági jogorvoslat, illetve a Hatósághoz fordulás lehetőségéről tájékoztatással.

A **személyes adatok helyesbítésről, zárolásról, megjelölésről és törlésről** Önt, továbbá mindazokat értesítem, akiknek korábban az adatot adatkezelés céljára továbbítottam, kivéve akkor, ha az értesítés elmaradása az Ön jogos érdekét nem sérti.

Amennyiben az Ön helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesítem, a kérelem kézhezvételét követő 15 napon belül (legfeljebb azonban 1 hónapon belül) írásban vagy – az Ön hozzájárulásával – elektronikus úton közölöm elutasításom indokait és tájékoztatom Önt a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

Amennyiben **Ön tiltakozik a személyes adatai kezelése ellen**, a tiltakozást a kérelem benyújtásától számított 15 napon belül (legfeljebb azonban 1 hónapon belül) megvizsgálom és a

döntésemről Önt írásban tájékoztatom. Amennyiben úgy döntötök, hogy az Ön tiltakozása megalapozott, abban az esetben az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is - megszüntetem, és az adatokat zárolom, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesítem mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbítottam, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Abban az esetben megtagadom a kérés teljesítését, ha bizonyítom, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az Ön érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Amennyiben Ön a döntésemmel nem ért egyet, illetve ha elmulasztom a határidőt, a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül Ön bírósághoz fordulhat.

Az adatvédelmi perek elbírálása a törvényszék hatáskörébe tartozik, a per – az érintett választása szerint – az érintett lakhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható. Külföldi állampolgár a lakóhelye szerint illetékes felügyeleti hatósághoz is fordulhat panasszal.

Kérem Önt, hogy mielőtt a felügyeleti hatósághoz vagy bírósághoz fordulna panaszával – egyeztetés és a felmerült probléma minél gyorsabb megoldása érdekében – keressen meg.

Az adatkezelés során kiemelt figyelmet fordítok arra, hogy az alábbi **adatvédelmi és -kezelési elveket**, az adatvédelmi és -kezelési politikát magamra nézve kötelező erővel ismerjem el és kövessem.

- a személyes adatokat jogszerűen és tisztességesen, valamint az Ön számára átláthatóan kezelem.
- a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból gyűjtöm és azokat nem kezelem a célokkal össze nem egyeztethető módon.
- az általam gyűjtött és kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak, valamint csak a szükségesre korlátozódnak.
- Minden észszerű intézkedést megteszek annak érdekében, hogy az általam kezelt adatok pontosak és szükség esetén naprakészek legyenek, a pontatlan személyes adatokat haladéktalanul törlöm vagy helyesbítem.
- A személyes adatokat olyan formában tárolom, hogy Ön csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig legyen azonosítható.
- Megfelelő technikai és szervezési intézkedések alkalmazásával biztosítom a személyes adatok megfelelő biztonságát az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szemben.
- Az az Ön személyes adatait
    - az Ön előzetes tájékoztatáson alapuló és önkéntes hozzájárulása alapján és csakis a szükséges mértékben és minden esetben célhoz kötötten kezelem, azaz gyűjtöm, rögzítem, rendszerezem, tárolom és felhasználom.
    - egyes esetekben jogszabályi előírásokon alapján kötelező jelleggel kezelem, ilyen esetekben erre a tényre külön felhívom az Ön figyelmét.
    - bizonyos esetekben, az Adatkezelőnek, vagy pedig harmadik személynek fűződik jogos érdeke, például honlapunk működtetése, fejlesztése és biztonsága alapján kezelem.

Az adatkezelés során a személyes adatok kezelését, tárolását, továbbítását a **hatályos jogszabályok**nak (különösen az alábbiaknak) megfelelően, azokkal összhangban, valamint az Adatvédelmi irányelv 29. cikk szerinti Adatvédelmi Munkacsoport iránymutatásainak és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) által kialakított adatvédelmi gyakorlatnak megfelelően végzem.

- a természetes személyeknek a személyes adatok kezeléséről szóló az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény - (Info tv.)
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.)
- az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény - (Eker tv.)
- az elektronikus hírközlésről szóló 2003. évi C. törvény - (Ehtv)
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény (Fogyv tv.)
- a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény. (Pktv.)
- a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (Grtv.)

Adatvédelmi értelmező szótár

- adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
- személyes adat: bármely meghatározott, azonosított vagy azonosítható természetes személlyel [érintett] kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés.
- A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az Adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
- adatalany/érintett: bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
- különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.
- bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.
- adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.
- adatkezelő: az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
- adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).
- adatfeldolgozó: az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.
- érintett jogai: az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről. Az érintett kérheti adatai helyesbítését, bizonyos esetben törlését is, valamint törvényben meghatározott esetekben tiltakozhat személyes adatai kezelése ellen.
- az adatkezelés jogalapja: főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.

- hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében szükséges az írásos forma.
- megfelelő tájékoztatás: az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.
- tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
- adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.
- az adatkezelés elvei: a célhoz kötött adatkezelés követelménye (lásd alább), valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes, törvényes mivoltát.
- célhoz kötött adatkezelés: személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és - ha az adatkezelés céljára tekintettel szükséges - naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
- adattovábbítás külföldre: személyes adatok továbbítása EGT-n (Európai Gazdasági Térség: az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz.
- információszabadság: a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, mely elősegíti a közhatalom gyakorlásának társadalmi kontrollját és a közintézmények működésének, valamint a közpénzek elköltésének átláthatóságát (transzparencia).
- közérdekű adat: az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).
- közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. (pl. a hitelezői érdekek védelme, valamint a piaci forgalom biztonsága érdekében az adatok széles körét minősíti közérdekből nyilvánosnak az ingatlan-nyilvántartásról szóló törvény, a cégtörvény, valamint a számviteli törvény)

- Avtv.: 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, a rendszerváltás utáni első adatvédelmi törvény, mely 2011. december 31-ig volt hatályban. 2012. január 1-től hatályon kívül helyezte az Infotv. (lásd alább).
- Infotv.: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, amelyet az Alaptörvény VI. cikke alapján az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, az ezen jogok érvényesülését szolgáló alapvető szabályokról, valamint az ellenőrző hatóságról (NAIH) alkotott. A törvény célja, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2012. január 1-től hatályos.
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- EDPS (European Data Protection Supervisor): a 2004-ben létrejött európai adatvédelmi biztos független intézményként felügyeli az európai intézményekben és uniós szervekben folyó személyes adatok kezelését, emellett az európai adatvédelmi joggyakorlat és jogértelmezés kialakításában is kulcsszerepe van.
- belső adatvédelmi felelős: az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős.
- Európa Tanács Adatvédelmi Egyezménye: az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon kihirdette az 1998. évi VI. törvény, 1998. február 27-én.
- uniós adatvédelmi irányelv: az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Európai Unió 1995. október 24-én született általános adatvédelmi irányelve, mely – többek között – létrehozta az ún. 29-es Adatvédelmi Munkacsoportot (lásd alább).
- 29-es Munkacsoport: A 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.
- uniós adatvédelmi szabályozás-tervezet (Data Protection Regulation – the „Proposed Regulation"): a jogi csomagként 2012-re előkészített anyag egyrészt magában foglalja az általános uniós adatvédelmi rendelet tervezetét (lásd alább), valamint a rendőrségi és bűnügyi igazságügyi adatkezeléseket szabályozó irányelv tervezetét.
- uniós adatvédelmi rendelet-tervezet: az Európai Bizottság 2012. január 25-én közzétett javaslata, melynek célja az európai adatvédelmi szabályok átfogó reformja és ennek keretében egy uniós szinten egységesebb, egyszerűbb és korszerűbb szabályozás kialakítása az európai polgárok adatainak kezelése érdekében. A rendelet, mint jogforrás (az irányelvtől eltérő módon) közvetlenül hatályosul az uniós tagállamokban, ami a tényleges, azonnali és

feltétlen jogharmonizációt garantálja uniós szinten. A tervezetet először a tagállamok és az Európai Parlament is megvitatja, majd, ha az Európai Parlament elfogadja, két év szükséges a hatályba lépéshez.

- Schengen/SIS: a schengeni térség létrehozása a személyek szabad mozgását lehetővé tevő legfontosabb uniós vívmány. A belső határok eltörléséből és a külső határok megszigorított ellenőrzéséből eredő biztonsági kockázatokat a Schengeni Információs Rendszer (SIS), Európa legnagyobb informatikai rendszere hivatott kezelni, elsősorban a hatékony adatmegosztás eszközével. A tagállamok keresett és eltűnt személyekkel, ellopott vagy elveszett tulajdonnal, beutazási tilalmakkal kapcsolatos adatokat – úgynevezett figyelmeztető jelzéseket – helyeznek el a SIS-ben. Az érintettek SIS-sel kapcsolatos adatvédelmi kéréseikkel (például tájékoztatási vagy helyesbítési kérelem) bármely rendőrkapitánysághoz vagy magyar külképviselethez fordulhatnak, akik ezt továbbítják az ORFK NEBEK SIRENE Irodához. A magyar SIS adatkezelések jogszerűségét a NAIH felügyeli.
- EURODAC: (European Dactyloscopy); a 2725/2000/EK rendelet által életre hívott európai ujjnyomat nyilvántartó adatbázis, melynek elsődleges célja a menedékkérők és illegális migránsok beazonosítása.
- OECD irányelvek: a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvei, melyek 1980. szeptember 23-án léptek életbe.
- BCR (Binding Corporate Rules – Kötelező Erejű Vállalati Szabályok): multinacionális társaságok által alkalmazott és a bejegyzés székhelye szerinti EU-tagállam adatvédelmi hatósága által jóváhagyott kötelező magatartási kódex. Ennek értelmében a multinacionális cégcsoport vállalja, hogy a vállalatcsoporton belüli, az EU tagállamok területéről harmadik, nem uniós országba történő adattovábbítás során megfelelő, a célországban egyébként szokásosnál nagyobb szintű védettséget biztosít az általa továbbított személyes adatoknak.
- ACTA (Anti-Counterfeiting Trade Agreement – Hamisítás elleni kereskedelmi megállapodás): nemzetközi megállapodás, melynek deklarált célja az interneten terjedő kalóztartalmakkal szembeni hatósági fellépés lehetőségének megteremtése. A megállapodás hivatalos előterjesztője Japán volt, a dokumentum 2011 márciusában nyílt meg aláírásra. A megállapodás létrehozására irányuló nemzetközi tárgyalások folyamán az európai adatvédelmi biztos (EDPS) 2010 februárjában kiadott véleményében a dokumentum uniós adatvédelmi szabályokkal való összeegyeztethetőségével kapcsolatban aggályát fejezte ki - az Európai Unió nem csatlakozott hozzá.
- BAR-lista: a magyar Központi Hitelinformációs Rendszer (KHR) korábbi elnevezése. A KHR a lakossági banki ügyfelek vonatkozásában két alrendszerből áll. A negatív listás alrendszerben található a késedelmes adósok hitelmulasztással kapcsolatos adatai, míg a pozitív listás rendszer tartalmazza valamennyi magyarországi hitelfelvevő, hitelintézetek által átadott ügyfél- és szerződésadatait. Ez utóbbi alrendszerből a bankok hiteltörténeti adatokat csak abban az esetben hívhatnak le, ha a hozzájuk forduló hiteligénylő a hitelképességének pontosabb megítélése érdekében ehhez kifejezetten hozzájárul.
- CCTV (Closed-Circuit Television): zárt láncú televíziós megfigyelési rendszer, mely több kamerából áll, és amelynek célja egy adott terület biztonsági célú állandó megfigyelése. Ellentétben a nyilvánosan közvetített, „nyílt láncú" televíziós adásokkal, a CCTV felvételei csak egy zárt csoport számára (általában a biztonsági személyzetek számára) nyilvánosak. A CCTV-rendszerek széleskörű elterjedése vitákat váltott ki a személyhez fűződő jogokat és adatvédelmet érintő esetleges negatív következmények miatt.

- PNR (Passenger Name Records): a légiutas-nyilvántartási adatállomány elsősorban az utas által a foglalás során megadott és a légitársaság által az utazással összefüggésben összegyűjtött adatokból áll, melyeket a légitársaságok és a repülőtéri irányító központok tárolnak, azonban ezekhez bűnüldöző hatóságok is bizonyos esetekben hozzáférést kapnak, kaphatnak. Az adatok kezelésének uniós szabályozása jelenleg is folyamatban van, az egyes adatvédelmi kérdések különös megfontolásokat igényelnek. A korábban sok vitát kiváltó, a légi utasok adatcseréjéről szóló, az EU és az Egyesült Államok közötti egyezmény 2012. július 1-én lépett hatályba.
- cloud computing: („számítástechnikai felhő", „felhő alapú informatika"): a számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (pl.: Gmail), vagy az online tárhelyek (pl.: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.
- cookie-k („sütik"): rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai.
- privacy by default: olyan adatvédelmi irányzat, melynek lényege, hogy személyes adatok gyűjtésére, kezelésére, illetve feldolgozására csak és kizárólag az adatalany kifejezett kérésére kerülhet sor. Az adatkezelők alapvető, „alapértelmezett" (angolul: by default) hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszik az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során.
- privacy by design: Kanadában, az 1990-es években kialakult adatvédelmi irányzat. Lényege, hogy az adatvédelmi szempontoknak megfelelő gyakorlat nem merülhet ki a hatályos szabályozásnak való formális megfelelésben. Az adott szervezet alapvető működési elve az adatvédelmi szempontoknak való megfelelés, ezért működését, struktúráját ezek maximális

figyelembevételével alakítja ki, az adatvédelmi szempontokat már az egyes működési fázisok megtervezésekor beépíti és így biztosítja az adatvédelem teljes körű érvényesülését. Rokon területe a „privacy by default" megközelítésnek.