

Data Protection Notice

regarding the processing of data in civil procedures under the jurisdiction of the Regional Court of Debrecen (in hungarian: Debreceni Ítéltábla) operating in its territorial jurisdiction

The Regional Court of Debrecen in its territorial jurisdiction (hereinafter: Court) pay(s) particular attention to conduct its(their) procession of data pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: GDPR),¹ Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Info. Act.), and other relevant legislations.

The processing carried out by the courts in the performance of their judicial tasks can be separated into two groups based on the data protection legislation applicable. This separation conforms to the two main fields the judicial practice is divided into based on branches of law: civil procedures and criminal procedures. The term ‘civil procedure’ encompasses cases under civil law, business law, administrative law and labour law (hereinafter collectively referred to as: civil procedures). The term ‘criminal procedure’ encompasses apart from cases under criminal law, cases of petty offences (falling under the scope of Act II of 2012 on the substantive and procedural rules of petty offences, and on the registry of petty offences) and cases of penal enforcement as well (hereinafter collectively referred to as: criminal procedures).

In civil procedures the processing of personal data is governed by the GDPR. Furthermore, the Info. Act. determines its provisions that should be applied [Section 2(2) of the Info. Act]. These provisions of the Info. Act regulate how data subjects can raise claims; definitions not contained in the GDPR; rules ensuring the freedom of information; rules on certain mandatory processing activities, as well as the organizational rules of the National Authority for Data Protection.

Pursuant to point d) of Article 2(2) of the GDPR, the Regulation does not apply to processing activities carried out in criminal procedures, the other main area of judicial activity. However, Section 2(3) of the Info. Act. states that its provisions shall be applied to the processing of data carried out for the purpose of law-enforcement, national security or national defence.

In accordance with Articles 13 and 14 of the GDPR, this Notice was prepared to provide information on the processing carried out by the Court in civil procedures.

For the purposes of this Notice:

data subject means – regardless of whether they participate in a contentious or non-contentious civil procedure – the parties, the witness, the expert, the possessor of an inspected document or item, and all those whose participation in the taking of evidence is deemed necessary by the court (hereinafter collectively referred to as: participating individuals), as well as any natural persons who are identified or are identifiable from the case files;

personal data means any information relating to a data subject;

sensitive data means data included in the special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, furthermore, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation;

personal data processed in criminal matters means personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

controller shall mean the Court processing personal data related to a data subject;

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

processing of data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The information to be provided can be found below in the order that is laid down in Articles 13 and 14 of the GDPR. Article 13 regulates information to be provided where personal data are collected from the data subject, while article 14 regulates information to be provided where personal data have not been obtained from the data subject.

1. Name of the controller

Regional Court of Debrecen (Debreceni Ítéltábla)
 President: Szilágyiné dr. Karsai Andrea
 Seat: 4025 Debrecen, Széchenyi utca 24.
 Postal address: 4001 Debrecen, Pf. 661.
 Phone: +36-52-527-972
 Fax: +36-52-528-017
 E-mail: birosag_dit@birosag.hu

2. Contact details of the local Data Protection Officer

Phone: +36-52-527-971
 E-mail: ditadatvedelem@birosag.hu
 Postal address: 4001 Debrecen, Pf. 661

3. Purpose of data management

The purpose of the data management is to assess the right asserted in the lawsuit in litigation and non-litigation proceedings for the decision of the court in the civil case, such as the conduct of procedures, the execution of the final decision after the final conclusion of the procedure, the verification of the contents of the final decision, the implementation of legal remedies related to the final decision or other tasks defined by law.

4. Scope of managed data

Scope of data processed for the above purposes:

- identification data of the person concerned;
- depending on the nature and subject of the given procedure, other personal data necessary to clarify the facts, including the special categories of personal data according to Article 9, Paragraph 1 of the GDPR, including the special data defined the Info Act. in Section 3, Point 4 of the Info Act, as well as criminal personal data according to Article 10 of the GDPR, defined in § 3, point 6 of

5. Legal basis for data management

The data management is based on Article 6(1)(e) of the GDPR, it is necessary for the execution of its tasks within the framework of the exercise of the public powers conferred on the Court, with regards to Article 25 (1)-(3) of the Basic Law and powers defined in § 1 of Act CLXI(Bszi.) of 2011 on the organization and administration of courts.

In the case of handling special categories of personal data, the condition that ensures it is based on point f) of Article 9 (2) of the GDPR.

In case of the decisions in connection with the setting up the criminal liability and criminal cases the assuring requirement is based on the 10. Article of the GDPR, assuming that the data are being processed under the control of the Court as a public authority.

6. Source of personal data

The Court handles personal data that have been made available to the Court either by the person concerned or by other bodies and persons.

If the personal data was not obtained by the Court from the person concerned, they may be processed by the Court from the following sources:

- from the person submitting the statement of claim or other request to initiate the procedure;
- from the party with an adverse interest in the proceedings;
- from a person participating in the procedure as a contributor;
- from the contacted body or organization, if the Court takes measures to obtain the document or data it possesses;
- from a public register regulated by law;
- through official knowledge.

7. Recipients of personal data and categories of recipients

For the purpose of judging the right asserted in the lawsuit, the court may process personal data acquired in connection with it after the final conclusion of its proceedings only for the purpose of implementing the final decision, checking the contents of the final decision, redressing the final decision or performing other tasks defined by law, and may only forward this personal data to another body or person authorized to process it [Code of Civil Procedure CXXX of 2016 (Pp.) § 162 (6)].

In this context, if the exercise of rights by the person concerned during the procedure is based on the data processing operation of the Court that implements the data protection incident, the data protection officer of the Court informs the data protection officer of the National Court Office about the data protection incident that has occurred.

Case files that cannot be discarded according to the document management rules will be handed over to the Hungarian National Archives (1014 Budapest, Bécsi kapu tér 2-4.).

In connection with the communication of paper-based case files by delivery, the personal data necessary for this will be transferred to Magyar Posta Zrt. (1138 Budapest, Dunavirág utca 2-6.).

In the case of regulated electronic contact and central electronic administration services, personal data is transferred to NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (1081 Budapest, Csokonai u. 3.).

Regarding the data transmitted via the electronic mail system, the National Court Office (1055 Budapest, Szalay u. 16.) acts as the operator of the mail servers as a data processor.

In addition, in individual cases, the Court communicates personal data to other bodies, which are not regarded as recipients for the purposes of its own or another body's exercise of public authority. Public authorities which may receive personal data in the framework of a particular inquiry shall not be regarded as recipients [Article 4 (9) of GDPR].

Such bodies may include in particular:

- the real estate regulatory authority;
- the Constitutional Court;
- the Court of Justice of the European Union;
- the European Court of Human Rights;
- the Ministry of Justice;
- in the case of initiating an administrative authority procedure for the review of the data classification, the National Authority for Data Protection and Freedom of Information (Falk Miksa Street 9-11, Budapest, 1055);
- the bodies or organizations requested during the procedure, if requesting such body or person is necessary in the given procedure for the clarification of the facts or the decision making, besides, the Court may disclose personal data to the extent strictly necessary to comply with the request;
- in the case of classified data, the request of the classifier according to Article 11 of Act CLV of 2009 on the Protection of Classified Data;
- depending on the nature of the claim, the transfer of enforcement-related data to an independent court officer or the National Tax and Customs Administration.

In addition, the Court will not communicate personal data to any other recipient when dealing with the request of the data subject. The data will not be transferred to third countries or international organizations.

8. Storage period of personal data

The Court shall process personal data disclosed with regard to the proceedings and with a view to deciding on the right enforced in the proceedings until the purpose of data processing is achieved, but no later than the discarding or archiving the documents of the case subject to the proceedings. [Section 162 (6) of the Code of Civil Procedure]

The written personal data processed in the proceedings are contained in a case file. In addition to the case file, non-written data (e.g. images and sound recordings) may be processed. If an annex to the file cannot be attached to the case file, it shall be preserved in accordance with the rules on written evidence [Section 30 (1) of the Instruction on Court Records Management]

The Court shall register case files in accordance with the rules governing the management of documents² and shall keep them among the registered documents for a certain storage period specified

² Main rules on document management:

- Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives (hereinafter: Act on Public Records)

in the filing plan in force or, failing that, until discarding or archiving them. Subsequently, with the exception of the data contained in the documents to be archived pursuant to the Act on the Public record, and the data to be processed by operation of law, the Court shall delete the data (discard the documents) or, with the archiving, the processing of personal data at the Court shall cease.

9. Rights of the data subject regarding data processing

In the case of data processing carried out in the course of the judicial activities of the Court, the data subject may exercise its rights granted by the GDPR to the extent that their exercise is not restricted by the rules governing the procedure in question.

The exercise of the data subject's right is required to be made in a request submitted in the case in accordance with the rules governing the procedure in question. The request is examined by the judge or judicial employee hearing the case.

9.1 Time limit

The time limit for the Court to deal with the request for exercising the rights of the data subject shall be the time limit established in the procedure in question. The Court shall inform the data subject of the action taken or the reasons for which not action has been taken.

9.2. Data subjects' rights in relation to data processing

9.2.1 Right to access

The data subject shall be entitled to obtain information whether his data are being processed and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint according to Chapter VI/A of the Privacy Act;
- where the personal data are not collected from the data subject, any available information as to their source.

On request by the data subject, the Court shall, within the aforementioned limits, provide a copy of the personal data undergoing processing.

To meet data security requirements and to protect the rights of the data subject, the Court shall verify that the identity of the data subject and that of the person wishing to exercise his or her access rights match. Therefore, obtaining information, consulting data or obtaining copies thereof requires the verification of the identity of the data subject. To the right to obtain copies, however, there is a limit: exercising this right should not adversely affect the rights or freedoms of others.

- Government Decree No. 335/2005 (XII. 29.) on the General Requirements of Document Management by Bodies Performing Public Duties
 - Government Decree No. 451/2016 (XII. 19.) on the Detailed Rules of Electronic Administration
 - Decree No. 14/2002 (VIII. 1.) of the Minister of Justice on the Rules of Court Administration (hereinafter: Decree on Rules of Court Administration)
 - Instruction No. 17/2014 (XII. 23.) of the National Court Office on the Uniform Rules on Court Records Management (hereinafter: Instruction on Court Records Management)

Laws on proceedings contain rules on the access to case files and, by regulating the related tasks of the court registries, Sections 10 to 12 of the Regulation No. 14 of 2012 on the Case Management of the Courts issued by the Minister of Justice lay down the rules of its practical realisation. These rules constitute limits to the right to access.

To the access to classified information the regulations of the Act CLV of 2009 on the Protection of Classified Information apply, according to which the classifier is authorized to grant access permission to the data subject. In addition, confidentiality rules may set further limits to the access to case files.

9.2.2. Right to rectification

The data subject shall, within limits set by the rules of the proceedings, have the right to obtain from the Court without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

9.2.3. Right to restriction of processing

The data subject shall have the right to obtain from the Court restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject (in this case the Court restricts processing for a period enabling it to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing (in this case restriction applies for the period during which the verification whether the legitimate grounds of the controller override those of the data subject).

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. Processing in civil cases is specifically related to the establishment, exercise or defence of legal claims, therefore the right to restriction of processing does not interfere with the processing carried out by the Court.

A data subject who has obtained restriction of processing based on the above shall be informed by the Court before the restriction of processing is lifted.

9.2.4. Right to object

The data subject shall have the right to object to processing of data for reasons relating to his or her particular situation. In this case the Court shall demonstrate the compelling legitimate grounds for the processing of the personal data which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. However data processing in civil cases are connected expressly to establishment, exercise or defence of legal claims.

9.2.5. Right to erasure

The data subject may exercise the right to erasure regarding to data processing stated in this guide, only if it is not necessary for the Court for the performance of a task carried out in the exercise of official authority vested in the Court or for public interest furthermore for the establishment, exercise or defence of legal claims [GDPR Article 17 Paragraph 3 Point b) and e)]. In civil cases it is fundamentally

possible for data processing after the period for which the processed personal data will be stored has expired.

In case of the above mentioned terms the data subject should have the right to obtain from the Court the erasure of personal data concerning him or her without undue delay. The Court should be obliged to erase the personal data concerning the data subject without undue delay where one of the following grounds apply:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject objects to the processing pursuant to the right of objection and there are no overriding legitimate grounds for the processing,
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

10. Right of remedy

Supervising the enforcement of the right to protection of personal data in connection with processing operations carried out by the Court in accordance with the relevant regulations in litigation and non-litigation proceedings aiming court decisions shall be exercised by means of data protection objection.

An objection may be submitted in writing to the court of original process addressed to the court of competence pursuant to the rules of the concrete procedure.

An objection may be submitted by the party and other parties to the proceedings - in particular the aggrieved party, the civil party, the witness and the expert – and any person who is able to prove his or her legal interest when submitting the objection

The data subject may submit the objection claiming that

- an alleged infringement took place in relation to the processing of his or her personal data or an immediate danger of infringement exists and
- the Court acted in an illegal way exercising the data subject's right regulated in the GDPR. In this case the data subject shall display the data corroborating that he or she attempted to exercise his or her rights of data subjects before the controller.

Based on the objection the court shall examine whether the judge, lay assessor or judicial staff acted in compliance with the legal provisions and European Union law applicable to the protection of personal data in their data processing operations.

If the court of original process deems the objection substantiated it shall take appropriate measures for mitigating the consequences of the infringement or to dismiss the danger within eight days, at the same time the court shall notify the person who submitted the objection thereof and the measures taken. The court shall inform this person that if he or she wishes to uphold the objection despite the measures taken, he or she may submit that statement in writing within eight days of receipt.

If the court of original process did not take any measures specified above or the data subject submitted the statement specified above, the court of original process shall forward the relevant documents within eight days to the court of jurisdiction to hear the objection.

If the court hearing the objection did not reject or dismiss the objection, it shall be decided on the merits by way of a reasoned decision within 2 months of receiving the relevant forwarded documents.

The objection submitted during a procedure shall be decided on the merits even if the litigation or non-litigation procedure has already concluded.

In addition to the above if you deem that the Court infringed the operative rules of data protection during processing your personal data, you may bring the case before court in order to protect your data. You may decide freely whether to file a claim before the competent regional court by reference to your home address or habitual residence or the registered office of the controller.

Before bringing the case to the National Authority for Data Protection and Freedom of Information or a court it is advisable to present the alleged infringement stated in the objection or in the claim in order for the controller to restore the lawful state within its own competence.