Data Protection Notice
regarding the processing of data in criminal procedures under the jurisdiction of the Regional Court of Debrecen (in hungarian: Debreceni Ítélőtábla) operating in its territorial jurisdiction

The Regional Court of Debrecen operating in its territorial jurisdiction (hereinafter: Court) pay(s) particular attention to conduct its(their) procession of data pursuant to 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 Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: GDPR).[1] 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 Section 16 of the Info Act., this Notice was prepared to provide information on the processing carried out by the Court in criminal procedures.

For the purposes of this Notice:
data subject means – regardless of whether they participate in a contentious or non-contentious criminal procedure – the defendant, the victim, 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 that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images);
recipient means a natural or legal person, and/or unincorporated organization, to which the personal data are made accessible by the data controller and/or the data processor.

The information to be provided can be found below in the order that is laid down in Section 16 of the Info Act.

1. Name of the controller

Regional Court of Debrecen (Debreceni Ítélőtábla)
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 conduct litigation and non-litigation procedures for reaching a court decision in a criminal case, to implement the final decision after the final conclusion of the procedure, to check the contents of the final decision, to implement 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 (1) of the GDPR, including special data defined in § 3, point 4 of the Info Act, and also criminal personal data defined in § 3, point 6 of the Info Act, according to Article 10 of the GDPR.

5. Legal basis for data management

Data management with regard to personal data is based on § 5, paragraph (1), point a) of the Info Act, it is ordered by law for purposes based on public interest.

The handling of special data and criminal personal data is based on § 5, paragraph (2) point b) of the Info Act, it is ordered by law in order to prevent, detect or prosecute crimes.

These legal provisions are § 97, paragraph (1) and § 98, paragraph (3) of Act XC of 2017 on criminal procedure (hereinafter: Be.), and § 76 of the CCXL Act of 2013 on the implementation of punishments, measures, certain coercive measures and detention for violations of the rules (hereinafter: Bv tv.).

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 were not obtained by the Court from the person concerned, they may be processed by the Court from the following sources:

• from the investigative authority;

• from the prosecutor's office;

• from the private prosecutor or substitute private prosecutor;

• from the victim/private party;

• 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, or from another register or database;

• from a notification made regarding other data collection activities;

• through official knowledge.

7. Recipients of personal data and categories of recipients

If the exercise of the data subject's rights is based on the data processing operation of the Court that implements the data protection incident, then 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 accordance with the provisions of Act XLVII of 2009 (Bnytv.) on the criminal registration system, on the registration of judgments handed down against Hungarian citizens by the courts of the member

states of the European Union, and on the registration of criminal and law enforcement biometric data, the Court informs the criminal registration body of the accused about the data specified there.

In addition, in individual cases, the Court communicates personal data to other bodies for the purposes of its own or another body's exercise of public authority.
Such bodies may include in particular:
- the investigating authority;
- the public prosecutor's office;
- 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 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 documents[2] and shall keep them among the registered documents for a certain storage period specified 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

[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)
- 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)

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 Privacy Act 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 enforced by 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.

If there are reasons to assume that the person submitting a request for the enforcement of the rights set out below is not identical to the data subject, the Court shall fulfil the request after verifying the identity of the person submitting the request [Article 15(4) of the Privacy Act].

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, but a maximum of 25 days. 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 request information whether his data are being processed by the Court itself or by the processor acting on behalf of, or instructed by, the Court. If such processing takes place, he shall be entitled to access his personal data as well as the information concerning
- the source of the personal data processed,
- the purpose and the legal basis of processing,
- the scope of the personal data processed,
- in the event of the transfer of the personal data processed, the scope of the recipients of the data transfer, including recipients in third countries and international organizations,
- the period of retention of the personal data processed, as well as the criteria for determining this period,
- the rights to which the data subject is entitled under this Act, as well as the method of their enforcing them,
- the existence of profiling when it is applied and
- the circumstances of any personal data breaches that might have occurred in the context of processing the data subject’s personal data, as well as their effects and the measures taken to address them.

The Court may, in proportion to the desired objective, restrict or reject the enforcement of the data subject’s right to access if this measure is absolutely necessary for securing any of the following interests:
- efficient and effective conduct of inquiries or proceedings carried out by or with the participation of the controller (in particular criminal proceedings),
- efficient and effective prevention and detection of criminal offences,
- enforcement of penalties and measures applied against the perpetrators of criminal offences,
- efficient and effective protection of public security,
- efficient and effective protection of the state’s external and internal security, in particular national defence and national security or
- protection of the fundamental rights of third parties.

In the event of applying a measure restricting or rejecting the enforcement of the data subject’s right to access, the Court shall notify the data subject in writing, without delay

- of the fact that the access has been restricted or rejected and of the legal and factual reasons thereof, if providing the data subject with such information does not impair the enforcement of an interest specified above,
- of the rights the data subject is entitled to under this Act, and of the method of their enforcement.

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 and Sections 15 to 27 of the Regulation No. 12. of 2018 (VI. 12.) 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

If the personal data processed by it are inaccurate, incorrect or incomplete, the Court shall, in particular upon the data subject's request, without delay, further specify or rectify them or, if it is compatible with the purpose of processing, supplement them with further personal data provided by the data subject or with a declaration attached by the data subject to the personal data processed, (hereinafter jointly "rectification").

The Court shall be exempted from this obligation if

- the accurate, correct or complete personal data are neither available nor provided by the data subject, or
- the authenticity of the personal data provided by the data subject cannot be verified beyond doubt.

If the Court rectifies personal data processed by it or by the processor acting on its behalf or by its order, it shall notify the controller having transferred the personal data affected by the rectification of the fact of rectification and of the rectified personal data.

9.2.3. Right to the restriction of processing

During the period of the restriction of processing, the Court or the processor acting on its behalf or by its order may, in addition to storage, perform processing operations with the personal data affected by the restriction, only for the purpose of enforcing the data subject's lawful interests or according to the provisions laid down in an Act, an international agreement or a binding legal act of the European Union.

To enforce the right to the restriction of processing, the Court shall restrict processing to the processing operations specified above,

- if the data subject contests the accuracy, correctness or completeness of the personal data processed by the Court or by the processor acting on its behalf or by its order, and the accuracy, the correctness or completeness of the personal data processed cannot be verified beyond doubt, for a period enabling the existing doubt to be clarified,

- for the period of the existence of the lawful interests that justify refraining from their erasure, if, due to the unlawfulness of the data processing, the data should be erased but, based on the data subject's written declaration or the information available to the Court, there are reasonable grounds to assume that the erasure of the data would violate the lawful interests of the data subject,
- if, due to the unlawfulness of the data processing, the data should be erased but retaining the data as evidence is necessary during inquiries or proceedings (in particular in criminal proceedings) specified by law and carried out by or with the participation of the Court or another body with public-service mission, until the final conclusion of said inquiries or proceedings, either with administrative finality or with a final and binding effect,

- if, due to the unlawfulness of the data processing, the data should be erased, but for the purpose of fulfilling the documentation obligation it is necessary to retain the data for a period of 10 years.

In the first case mentioned above, in the event of terminating the restriction of processing, the data subject shall be informed by the Court before the restriction of processing is lifted.

9.2.4. Right to erasure

Personal data and protected data processed in the criminal proceeding may be erased only in compliance with the provisions of the Act XC of 20167on the Code of Criminal procedure before the conclusion of the proceeding,

Unless otherwise provided by other legislation the personal data processed in compliance with Section 76-78. of Act CCXL of 2013 on the Enforcement of Penalties, Measures, Certain Coercive Measures and Detention for Misdemeanours shall be erased at the time of enforcement or expiration of enforceability of penalty, measure, coercive measure or confinement for an infraction.

In order to exercise the right of erasure the Court respects these rules and shall erase the personal data of the data subject without delay if
- the processing is unlawful, in particular if the processing
    - is in contradiction with the principles laid down in Section 4.
    - the purpose of processing no longer exists, or further processing is not required for achieving the purposes of the processing,
    - the period specified by law, in an international agreement or binding legislation of the European Union has expired or
    - the legal basis for processing no longer exists, and no other legal basis applies;
- the data subject has withdrawn his or her consent on which the processing is based, or requests the erasure of his or her personal data, except if processing is mandatory or where processing is necessary and proportionate for protecting the vital interests of the data subject or of another person, or in order to prevent or avert an immediate risk of damage to lives, physical integrity or property of persons;
- the erasure of the data was ordered by law, any legislation of the European Union or a court; or
- the period of restriction specified by Paragraphs 2-4. has expired.

9.2.5. The obligation of providing information in relation to requesting rectification, erasure or restriction of data processing

If the court rejects the request for rectification, erasure or restriction of the data processing, the court shall inform the data subject in writing without delay
- the existence of the refusal, and its basis of the matters of law and matters of fact, and
- about the data subject's rights provided under this Act, and the manner to enforce them.

The court may delay, restrict, disregard the provision of information on the refusal, and the basis of the matters of law and of fact to a proportionate measure if this action is absolutely necessary in order to ensure any interest mentioned in point 9.2.1.

If the court rectifies, erases or restricts the processing of the processed personal data, the court shall notify the controllers and processors to whom such data was disclosed of this action and it's content, in order for them to execute the rectification, erasure or restriction of data processing concerning their own data processing.

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 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 Act on the Right of Informational Self-Determination and on Freedom of Information. 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 Court.

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 obligation.

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 the 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 adress 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 oder for the contoller to restore the lawful state within its own competence.