Croatian Implementation of the GDPR

by Marija Gregoric and Lovro Klepac, Babic & Partners, LLC, with Practical Law Data Privacy Advisor

Practice notes | Law stated as of 09-Apr-2021 | Croatia

A Practice Note discussing the requirements of Croatia's Implementation Act of the EU General Data Protection Regulation (GDPR) (in Croatian). This Note discusses the applicability of Croatian data protection law and key provisions of the law, such as rules for processing special categories of personal data, including biometric and genetic data, processing for secondary purposes, limitations on the scope of data subjects' rights, processing for official statistical purposes, and personal data processing in the employment context.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) took effect on May 25, 2018, replacing the EU Data Protection Directive (Directive 95/46/EC) (EU Directive) and the prior Croatian data protection law. The GDPR introduced a single legal framework across the EU. However, the GDPR includes several provisions allowing EU member states to enact national legislation specifying, restricting, or expanding some requirements.

Croatia enacted the Implementation Act of the EU General Data Protection Regulation (May 25, 2018) (in Croatian) (Croatian Act) which aligns Croatian data protection law with the GDPR. The Croatian Act also makes use of the GDPR's opening clauses and complements some of the GDPR's requirements.

This Note discusses the applicability of Croatian data protection law and key provisions of the Croatian Act, including requirements on:

- Processing special categories of personal data, including genetic and biometric data.
- Processing for secondary purposes.
- Limitations on data subjects' rights and controllers' and processors' related obligations when processing personal data for official statistical purposes.
- Processing in the employment context, including processing employee biometric data and using workplace video surveillance.
- Imposing administrative fines.

For guidance from the Croatian Personal Data Protection Agency, see GDPR Data Protection Authority Guidance Tracker by Country (EEA): Croatia.

Applicability of the GDPR and Croatian Law

The GDPR applies to:

- Controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU (Article 3(1), GDPR).
- Controllers and processors not established in the EU that process personal data about data subjects in the EU when the processing activities relate to:
    - offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment; or
    - monitoring data subjects' behavior that takes place in the EU.

  (Article 3(2), GDPR.)
- Controllers not established in the EU that process personal data and that are subject to EU member state law under public international law (Article 3(3), GDPR).

Some EU member states have passed national laws that include a territorial scope provision that mirrors GDPR Article 3. Other member states' laws include different applicability language or do not include a territorial scope provision. The Croatian Act does not include a provision stating the law's territorial scope.

Instead, the Croatian Act defines the scope of its application for certain types of processing, for example:

- The provisions on the age of child consent when providing information society services directly to the child only apply when the child resides in Croatia (Article 19(2), Croatian Act; see Child Consent).
- The provisions prohibiting processing genetic data in the context of entering into and performing life insurance contracts or contracts with endowment clauses apply when:
    - the data subject enters into the contract in Croatia; and
    - the controller is established in Croatia or provides services in Croatia.

    (Article 20, Croatian Act; see Genetic Data.)
- The provisions governing processing biometric data only apply to data subjects in Croatia if:
    - the controller is established in Croatia or provides services in Croatia; or
    - the controller is a public authority.

    (Article 24, Croatian Act; see Biometric Data.)

The provisions on processing biometric data do not apply to processing in the context of defense, national security, and intelligence activities (Article 24(3), Croatian Act).

The Croatian Act also expressly excludes from its scope personal data processing:

- By competent authorities for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, which are covered by the Law Enforcement Directive (EU Directive 2016/680) and special implementing legislation.
- In the context of protecting against and preventing threats to public safety.
- In the context of national security and defense.

(Article 1(2), Croatian Act.)

For more on the GDPR's applicability and scope, see Practice Note, Determining the Applicability of the GDPR.

Data Protection Officers

The GDPR requires controllers and processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). The Croatian Act does not require appointing a DPO under additional circumstances or change the requirements or obligations applicable to DPOs under the GDPR.

For more on appointing DPOs under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Appointment of a data protection officer and GDPR Data Protection Authority Guidance Tracker by Country (EEA): Croatia.

Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR). Special categories of personal data include:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health or sex life.
- Sexual orientation.

(Article 9(1), GDPR.)

GDPR Exceptions Permitting Processing

GDPR Article 9(2) includes several exceptions to the prohibition on processing special categories of personal data. Some of these exceptions require controllers to consult EU or member state law to determine a lawful basis for processing.

The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the controller's obligations and exercising the controller's or data subjects' rights in the fields of employment law, social security, and social protection (Article 9(2)(b), GDPR).
- Reasons of substantial public interest (Article 9(2)(g), GDPR).
- Purposes of preventive or occupational medicine, assessing an employee's working capacity, medical diagnosis, or for the provision of health or social care or treatment, the management of health or social care systems and services, based on EU or member state law or under a contract with a healthcare professional, subject to certain conditions and safeguards (Article 9(2)(h), GDPR).
- Reasons of public interest in the area of public health (Article 9(2)(i), GDPR).
- Archiving in the public interest, scientific or historical research purposes, or statistical purposes (Article 9(2)(j), GDPR).

Other GDPR Article 9 exceptions provide a sufficient legal basis for processing special categories of personal data without the need for a further basis in EU or member state law, including when the data subject consents to processing (Articles 9(2)(a), (c) to (f), GDPR).

EU or member state law may prohibit the use of data subject consent as a legal basis for processing special categories of personal data (Article 9(2)(a), GDPR). The Croatian Act prohibits the use of consent as a legal basis to process genetic data in the context of entering into and performing life insurance contracts or contracts with endowment clauses (Article 20(2), Croatian Act; see Genetic Data).

For more on processing special categories of personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data.

Croatian Act Exceptions That Permit Processing Special Categories of Personal Data

The Croatian Act only includes provisions introducing further restrictions, limitations, or requirements for processing genetic and biometric data (see Genetic Data and Biometric Data). All other processing relating to special categories of personal data must comply with GDPR Article 9 (see GDPR Exceptions Permitting Processing).

Genetic, Biometric, and Health Data

The GDPR permits EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR). The Croatian Act includes exceptions permitting the processing of genetic and biometric data (Articles 20 to 24, Croatian Act; Article 9(4), GDPR).

Genetic Data

The Croatian Act prohibits processing genetic data in the context of entering into and performing life insurance contracts or contracts with endowment clauses (Article 20(1), Croatian Act). This Article also expressly prohibits the use of consent as a legal basis to process genetic data for these purposes (Article 20(2), Croatian Act; Article 9(2)(a), GDPR).

The prohibitions in this Article only apply when both:

- The data subject executing the agreement is in Croatia.
- The controller is established in Croatia or provides services in Croatia.

(Article 20(3), Croatian Act.)

Violating the rules on processing genetic data under Croatian Act Article 20 constitutes a violation of GDPR Article 9 subject to administrative fines under GDPR Article 83(5) (Article 20(4), Croatian Act; see Administrative Fines).

Biometric Data

The Croatian Act includes specific rules governing the processing of biometric data by public- and private-sector entities, including in the employment context.

Private-sector entities may only process biometric data when either:

- Applicable law requires the processing.
- Data subjects' interests do not override the processing, which is necessary:
  - to protect individuals, property, classified information, or business secrets; or
  - for the individual and secure identification of service users (data subjects).

(Article 22(1), Croatian Act; Article 9(4), GDPR.)

Private-sector controllers must rely on service users' explicit consent as the legal basis for processing biometric data for the purpose of securely identifying service users (Article 22(2), Croatian Act).

Public authorities may only process biometric data when all of the following apply:

- Applicable law requires the processing.
- The processing is necessary to protect individuals, property, classified information, or business secrets.
- Data subjects' interests do not override the processing.

(Article 21(1), Croatian Act; Article 9(4), GDPR.)

Processing biometric data is deemed to be in compliance with the law when the processing is necessary to fulfill obligations arising under international treaties that relate to identifying individuals at state border crossings (Article 21(2), Croatian Act).

The Croatian Act also permits public- and private-sector employers to process biometric data under certain circumstances (Article 23, Croatian Act; Article 88, GDPR; see Employee Biometric Data).

Article 24 of the Croatian Act defines when the provisions on processing biometric data apply (see Applicability of the GDPR and Croatian Law).

Processing Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions or offenses when either:

- Carried out under the control of official authority, for example, the police.
- EU or EU member state law authorizes the processing and provides for appropriate safeguards for data subjects' rights and freedoms.

(Article 10, GDPR.)

The Croatian Act does not include a provision authorizing processing this data under additional circumstances. All processing relating to criminal conviction and offense data must comply with GDPR Article 10.

Processing for Secondary Purposes

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose (see GDPR Article 23 Objectives that Permit Restrictions to Data Subject Rights).

(Article 6(4), GDPR.)

The Croatian Act permits further processing of personal data for official statistical purposes under special rules governing official statistics. This processing is considered compatible with the original collection purpose. No other legal basis for processing is necessary, provided the controller implements appropriate safeguards to protect the data. (Article 33, Croatian Act; Article 6(4) and Recital 50, GDPR.)

The Croatian Act also permits secondary processing of data collected through video surveillance when used as evidence in judicial, administrative, arbitration, or other proceedings (Article 29, Croatian Act; see Video Surveillance).

All other secondary processing must comply with the GDPR's requirements for secondary processing under GDPR Article 6(4). Without data subject consent, the secondary processing purpose must be compatible with the original processing purpose. To determine the secondary processing purpose's compatibility, the controller should consider the criteria specified in GDPR Article 6(4).

For more on processing personal data for secondary purposes under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Purpose limitation.

Child Consent

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, provided the age is not lower than 13 (Article 8(1), GDPR). However, the Croatian Act does not reduce the age of child consent, change the requirements for obtaining valid consent from children, or impose any additional requirements or restrictions on processing personal data about children. Instead, the Croatian Act adopts the same language as GDPR Article 8(1) and requires consent for children under 16 (Article 19(1), Croatian Act).

Croatian Act Article 19, relating to the offer of information society services directly to a child, applies to children that reside in Croatia (Article 19(2), Croatian Act). A violation of Article 19 of the Croatian Act is a violation of GDPR Article 8 and is subject to sanctions under GDPR Article 83 (Article 19(3), Croatian Act, see Administrative Fines).

Data Subjects' Rights

The GDPR grants data subjects several rights and imposes several obligations on controllers and processors relating to those rights in Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) (see Practice Note, Data Subject Rights Under the GDPR). The GDPR permits EU member states to restrict the scope of these data subject rights and controllers' and processors' related obligations when the restriction is a necessary

and proportionate measure to safeguard certain objectives or in other specific processing situations (Articles 23 and 85 to 91, GDPR; see GDPR Article 23 Objectives that Permit Restrictions to Data Subject Rights and Derogations for Specific Processing Situations).

GDPR Article 23 Objectives that Permit Restrictions to Data Subject Rights

EU member states may restrict the scope of data subjects' rights and controllers' and processors' related obligations found in GDPR Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- Other important economic or financial public interests of the EU or member state, including:
    - monetary, budgetary, and taxation matters;
    - public health; and
    - social security.
- Judicial independence and judicial proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
    - national or public security;
    - defense;
    - other important public interests;
    - crime prevention; or
    - breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

EU or member state laws restricting data subjects' rights to ensure GDPR Article 23 objectives should include provisions on, when relevant:

- Purposes of the processing or categories of processing.
- Categories of personal data.
- Scope of the restrictions.
- Safeguards to prevent abuse or unlawful access or transfer.
- Specification of the controller or categories of controllers.
- Data retention periods and applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- Risks to the rights and freedoms of data subjects.
- Data subjects' rights to be informed about restrictions, unless doing so is prejudicial to the restriction's purpose.

(Article 23(2), GDPR.)

Croatian Act Variations to Data Subject Rights

The Croatian Act permits controllers to restrict certain data subject rights when the controller processes personal data for official statistical purposes under applicable laws. For more information, see Processing for Statistical Purposes.

Derogations for Specific Processing Situations

GDPR Articles 85 to 91 provide additional rules that apply to seven specific processing situations. These Articles permit EU member states to enact further rules that apply to the specified processing types. The Croatian Act introduces further rules that apply to:

- Processing for statistical purposes (see Processing for Statistical Purposes).
- Secrecy obligations (see Secrecy Obligations).
- Processing in the employment context (see Processing in the Employment Context).

Processing for Statistical Purposes

Under the Croatian Act, certain GDPR Articles relating to data subjects' rights and controllers' and processors' related obligations do not apply to processing for official statistical purposes, including:

- Access rights (Article 15, GDPR).
- Rectification rights (Article 16, GDPR).
- Processing restriction rights (Article 18, GDPR).
- Objection rights (Article 21, GDPR).

(Article 33(1), Croatian Act; Article 89(2), GDPR.)

Controllers and processors should only restrict these rights when both:

- Strictly necessary to achieve the official statistical purpose.
- Permitting data subjects to exercise their rights would likely impede or seriously jeopardize achieving the official statistical purpose.

(Article 33(1), Croatian Act.)

The Croatian Act does not require controllers to notify data subjects when transferring their personal data for statistical purposes to the authorities responsible for official statistics (Article 33(3), Croatian Act).

Controllers and processors processing personal data for statistical purposes must not allow data subject identification (Article 33(5), Croatian Act). Personal data processed for statistical purposes is also deemed compatible with the original collection purpose (Article 33(4); see Processing for Secondary Purposes).

Secrecy Obligations

The GDPR permits EU member states to adopt rules specifying the powers of supervisory authorities under GDPR Articles 58(1)(e) and (f) regarding controllers and processors that are subject to:

- An obligation of professional secrecy.
- Another equivalent secrecy obligation.

(Article 90, GDPR).

The Croatian Act requires controllers and processors processing information classified as secret under a special law to process it according to that law (Article 39(1), Croatian Act; Article 90, GDPR). Only officials holding a valid certificate to access classified information can access, copy, or otherwise process information classified as secret under a special law (Article 39(2), Croatian Act).

Processing in the Employment Context

The GDPR permits EU member states, by law or by collective agreements, to provide more specific rules on processing personal data in the employment context (Article 88, GDPR). The Croatian Act provides for more specific rules relating to:

- Processing biometric data about employees (see Employee Biometric Data).
- Using video surveillance in the workplace (see Workplace Surveillance).

Other Croatian laws also regulate employee data processing, for example, the Employment Act and the Occupational Safety Act (both in Croatian). These laws' requirements are outside the scope of this Note.

If another Croatian law also applies to data processing covered by the GDPR, the Croatian data protection authority or the courts must directly apply the GDPR's provisions if a conflict between the GDPR and another Croatian law

occurs (Article 288, Treaty on the Functioning of the European Union and Article 141.c, Croatian Constitution (in Croatian)).

Employee Biometric Data

The Croatian Act permits processing employees' biometric data for the purpose of recording working hours and logging entry and exit at the employer's premises, if the employee explicitly consents and either:

- Applicable law authorizes this processing.
- The employer conducts the biometric processing as an alternative to another solution for recording working hours and entry and exit, for example, using employees' IDs. Employees may choose between biometric processing for these purposes or the other solution offered.

(Article 23, Croatian Act; Article 88, GDPR).

Workplace Surveillance

The Croatian Act permits employers to use video surveillance in the workplace if they satisfy both:

- The Croatian Act's general requirements for lawful use of video surveillance (Articles 25 to 32, Croatian Act).
- The requirements for video surveillance in the Occupational Safety Act (Article 43, Occupational Safety Act).

For more, see Video Surveillance.

Other GDPR Derogations

Supervisory Authority

GDPR Article 54 requires each EU member state to establish a supervisory authority. Croatian Act Article 4 establishes the Croatian Data Protection Authority (Croatian DPA). In addition to the powers specified in GDPR Article 58, the Croatian Act grants the Croatian DPA additional powers to:

- Initiate and participate in criminal, misdemeanor, administrative, and other judicial and non-judicial proceedings for GDPR and Croatian Act violations, when prescribed by special laws.
- Adopt criteria for determining the administrative cost of:
    - repetitive or manifestly unfounded data subject requests; and
    - providing expert opinions to business entities like consultants and law firms, which request expert opinions in the course of their business operations or providing services.
- Publish decisions on certain GDPR and Croatian Act violations under Articles 18 and 48 of the Croatian Act.
- Initiate and conduct proceedings for violations of the GDPR and the Croatian Act.

- Perform the work of an independent supervisory authority to monitor application of the Law Enforcement Directive (Directive 2016/680), unless prescribed differently by special laws.
- Perform other tasks mandated by law.

(Article 6, Croatian Act; Article 58(6), GDPR.)

Administrative Fines

The GDPR permits EU member states to specify penalties for GDPR violations that are not subject to administrative fines under GDPR Article 83 (Article 84, GDPR). The Croatian Act specifies that certain violations are also deemed violations of the GDPR subject to administrative fines under GDPR Article 83, including:

- Violating the rules on the minimum age of consent when offering information society services to children constitutes a violation of GDPR Article 8 (Conditions applicable to child's consent in relation to information society services) (Article 19, Croatian Act; see Child Consent).
- Violating the rules on processing genetic data constitutes a violation of GDPR Article 9 (Processing special categories of personal data) (Article 20, Croatian Act; see Genetic Data).

Administrative fines of up to HRK 50,000 also apply to:

- Violations of Croatian Act Article 27, which requires the controller or processor to provide information on video surveillance.
- Violations of Croatian Act Article 28, which requires the controller or processor to establish an automated system for recording access to video recordings, including the time and place of access and the identity of the person gaining access.
- Any person using personal data collected by video surveillance for a purpose other than the lawful collection purpose.

(Article 51, Croatian Act; see Video Surveillance.)

For more on enforcement and sanctions under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 26 and GDPR Enforcement Tracker by Country (EEA): Croatia.

Public Authorities and Bodies

The GDPR permits EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies (Article 83(7), GDPR). Article 47 of the Croatian Act specifically exempts public authorities and bodies from administrative fines.

Complaints on Behalf of Data Subjects

The GDPR permits EU member states, in their national laws, to allow certain not-for-profit bodies, organizations, or associations to lodge a complaint with a supervisory authority independent of a data subject's authorization to lodge the complaint (Article 80(2), GDPR).

The Croatian Act does not permit these organizations to lodge a complaint independent of the data subject's mandate. However, it does permit data subjects to authorize one of these organizations to lodge a complaint with a supervisory authority on their behalf, if the organization:

- Is formed according to applicable laws.
- Has statutory objectives in the public interest.
- Is active in the field of protecting data subjects' rights and freedoms relating to their personal data.

When authorized by a data subject, these organizations may exercise the data subject's rights to:

- Lodge a complaint with a supervisory authority (GDPR Article 77).
- An effective judicial remedy against:
    - a supervisory authority (GDPR Article 78); or
    - a controller or processor (GDPR Article 79).
- Receive compensation under GDPR Article 82 for damages suffered from a GDPR violation.

(Article 41, Croatian Act; Article 80(1), GDPR).

Video Surveillance

The Croatian Act includes provisions on:

- Video surveillance generally.
- Surveillance of work premises.
- Surveillance of public areas and residential buildings.

(Articles 25 to 32, Croatian Act.)

The GDPR does not explicitly permit EU member states to introduce specific rules regulating video surveillance. However, GDPR Article 6(2) provides a legal basis for EU member states to introduce specific rules on video surveillance, including provisions applicable to storage periods, to the extent the use of video surveillance is necessary either:

- To comply with a legal obligation under GDPR Article 6(1)(c).
- To perform a task carried out in the public interest or to exercise the controller's official authority under GDPR Article 6(1)(e).

(Article 6(2), GDPR.)

GDPR Article 88 also provides a legal basis for member states to enact specific provisions on video surveillance in the workplace (see Workplace Surveillance).

When using video surveillance, the Croatian Act requires that:

- The controller only processes personal data collected through video surveillance for a purpose that is necessary and justified to protect individuals and property and provided data subjects' interests do not override the need for data processing through video surveillance (Article 26(1), Croatian Act).
- The controller or processor limit the video surveillance perimeter to the interior premises, parts of the interior premises, the exterior surface of the building or structure, or the interior of public transportation vehicles, the surveillance of which is necessary to protect individuals and property (Article 26(2), Croatian Act).
- The controller or processor provide data subjects with the information required by GDPR Article 13 (Information to be provided when collecting personal data from the data subject) and post a clear and understandable sign visible when entering the recorded area that includes:
    - notice that the premises are under video surveillance;
    - information on the controller; and
    - contact details for data subjects to exercise their rights relating to their personal data.

    (Article 27, Croatian Act.)
- Only the controller, processor, persons authorized by the controller or processor, or public authorities carrying out their duties may access personal data collected through video surveillance (Article 28(1), (5), Croatian Act).
- The controller, processor, or other persons authorized by them do not use the personal data for any purpose different from the lawful collection purpose (Article 28(2), Croatian Act).
- The controller or processor:
    - implement security measures to protect the video surveillance system from unauthorized use (Article 28(3), Croatian Act); and
    - establish an automated system for recording access to video recordings, including the time and place of access and the identity of the person gaining access (Article 28(4), Croatian Act).
- The controller or processor only retain video surveillance recordings for a maximum of 6 months, unless:
    - applicable law permits or requires a longer retention period; or
    - the recordings are used as evidence in a judicial, administrative, arbitration, or other proceeding.

    (Article 29, Croatian Act.)

Article 30 of the Croatian Act requires employers conducting workplace video surveillance to also comply with the Occupational Safety Act, which requires the controller or processor to:

- Refrain from installing video cameras in private areas, such as bathrooms or dressing rooms.
- Inform employees in writing before setting up video surveillance.
- Obtain the prior consent of the works council or union trustee (if appointed within the employer) when the video surveillance monitors all employee movements at work or the employers are under surveillance the entire workday.

(Article 43, Occupational Safety Act.)

Employers may only use video surveillance recordings for the purposes described in the Croatian Act and Occupational Safety Act.

The Croatian Act includes additional requirements applicable to video surveillance of residential buildings (Article 31) and public areas (Article 32). It limits video surveillance of public areas to public authorities, legal persons with public authority, and legal persons engaged in public service when the surveillance is:

- Mandated by law.
- Necessary to carry out the tasks and duties of public authorities.
- Necessary to protect human life, health, or property.

(Article 32(1), Croatian Act.)

Controllers using video surveillance in public areas must still carry out a data protection impact assessment if the controller satisfies the conditions under GDPR Article 35 (Article 32(2), Croatian Act; see Practice Note, Overview of EU General Data Protection Regulation: Data protection impact assessment).

Croatian Act and GDPR Statutory References

Subject Matter	Croatian Act Article	GDPR Article(s) Permitting Member State Derogation
Applicability of the Croatian Law (see Applicability of the GDPR and Croatian Law)	19(2), 20(3), 24	
Appointing a data protection officer (see Data Protection Officers)	N/A	37(4), 38(5)
Requirements for processing special categories of personal data (see Processing Special Categories of Personal Data)	See Genetic, Biometric, and Health Data	9(2)(b), (g), (h), (i), (j)
Requirements for processing genetic, biometric, and health data (see Genetic, Biometric, and Health Data)	20 to 24	9(4)
Requirements for processing criminal conviction and offense data (see Processing Criminal Conviction and Offense Data)	N/A	10

Processing for secondary purposes (see Processing for Secondary Purposes)	29, 33	6(4)
Child consent (see Child Consent)	19(1)	8(1)
Data subjects' rights (see Data Subjects' Rights)	See Processing for Statistical Purposes	23
Processing for scientific or historical research and for statistical purposes (see Processing for Statistical Purposes)	33	89(2)
Secrecy obligations (see Secrecy Obligations)	39	90(1)
Processing employee personal data (see Processing in the Employment Context)	23, 25 to 30	88
Supervisory authority (see Supervisory Authority)	4, 6 to 18, 34, 36 to 40, 42, 43	54
Administrative fines (see Administrative Fines)	19, 20, 44 to 51	84
Public authorities and bodies (see Public Authorities and Bodies)	47	83(7)
Complaints on behalf of data subjects (see Complaints on Behalf of Data Subjects)	41	80(1)
Use of video surveillance (see Video Surveillance)	25 to 32	6(2)

END OF DOCUMENT