# Croatian Implementation of the GDPR

MARIJA GREGORIC AND LOVRO KLEPAC, BABIC & PARTNERS, LLC, WITH PRACTICAL LAW DATA PRIVACY ADVISOR



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

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which took effect on May 25, 2018, applies directly in each EU member state. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) (EU Directive) and the prior Croatian data protection law. The GDPR introduces 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 the scope of the GDPR's 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. Organizations must understand how the Croatian Act's requirements vary and when they apply in addition to the GDPR.

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

- Processing special categories of personal data, including genetic and biometric data.
- Processing for secondary purposes.
- Limitations on data subjects' rights and data controllers' 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.

## APPLICABILITY OF THE GDPR AND CROATIAN LAW

The GDPR applies to:

- Data controllers and data 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).
- Data controllers and data processors not established in the EU that process personal data about EU data subjects when the processing activities relate to:
  - offering goods or services to EU data subjects, regardless of whether they require payment; or
  - monitoring their behavior in the EU.

  (Article 3(2), GDPR.)

Some EU member states have passed national laws that include a territorial scope provision that mirrors Article 3 of the GDPR, while other countries' laws have slightly modified the applicability language in this Article. The Croatian Act does not include a provision either restating or modifying the GDPR's Article 3 scope provisions or a general provision stating the territorial scope of the Croatian Act.

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 restricting processing genetic data in the context of entering into and performing insurance contracts applies when:
  - the data subject enters into the contract in Croatia; and
  - the data 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 data controller is established in Croatia or provides services in Croatia; or
  - the data controller is a public authority.

  (Article 24, Croatian Law; 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 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 Police Directive 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 (w-003-8899).

## DATA PROTECTION OFFICERS

The GDPR requires data controllers and data processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR; see Practice Note, Data protection officers under the GDPR and DPA 2018 (w-010-3427)). 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.

## 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

The GDPR permits organizations to process special categories of personal data when:

- The data subject explicitly consents to the processing (Article 9(2)(a), GDPR). GDPR Article 9(2)(a) permits EU or member state law to prohibit the use of explicit data subject consent as a legal basis for processing special categories of personal data.
- The processing is necessary for:
  - carrying out the data controller's obligations and exercising the data controller's or data subjects' rights in the field of employment law, social security, and social protection (Article 9(2)(b), GDPR);
  - protecting the vital interests of the data subject or another person and the data subject is physically or legally incapable of consenting (Article 9(2)(c), GDPR);
  - establishing, exercising, or defending legal claims or whenever courts are acting in their judicial capacity (Article 9(2)(f), GDPR);
  - reasons of substantial public interest (Article 9(2)(g), GDPR);
  - purposes of preventive or occupational medicine to assess the working capacity of a data subject, medical diagnosis, or for the provision of health or social care or treatment, the management of health or social care systems and services, or under a contract with a healthcare professional (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 (Article 9(2)(j), GDPR); or
  - scientific, historical research, or statistical purposes (Article 9(2)(j), GDPR).
- The processing relates to the legitimate activities of certain non-profit organizations, is based on appropriate safeguards, and relates to certain persons (Article 9(2)(d), GDPR).
- The processing relates to personal data made public by the data subject (Article 9(2)(e), GDPR).

#### Exceptions not Requiring a Basis in EU or Member State Law

Some exceptions to the prohibition on processing special categories of personal data do not refer to EU or member state law. These exceptions provide a sufficient legal basis for processing special categories of personal data under the GDPR without the need for a further basis in EU or member state law, including:

- Explicit consent. However, EU or member state law may prohibit the use of data subject consent as a legal basis for processing. (Article 9(2)(a), GDPR.)
- Processing necessary to protect a natural person's vital interests and the data subject is incapable of consenting (Article 9(2)(c), GDPR).
- Processing relating to the legitimate activities of certain non-profit organizations, based on appropriate safeguards, and relating to certain persons (Article 9(2)(d), GDPR).
- Processing relating to personal data made public by the data subject (Article 9(2)(e), GDPR).
- Processing necessary for establishing, exercising, or defending legal claims or whenever courts are acting in their judicial capacity (Article 9(2)(f), GDPR).

#### Exceptions Requiring a Basis in EU or Member State Law

The other GDPR Article 9 exceptions permitting processing refer to EU or member state law and require data controllers to consult EU or member state law to determine the lawful basis for processing under these Articles. The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the data controller's obligations and exercising the data controller's or data subjects' rights in the field 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 to assess the working capacity of a data subject, medical diagnosis, or for the provision of health or social care or treatment, the management of health or social care systems and services, or under a contract with a healthcare professional (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).

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 (w-007-9580).

### 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, which implement GDPR Article 9(4)).

#### Genetic Data

The Croatian Act prohibits processing genetic data to assess data subjects' illnesses or other health aspects relating to concluding or performing a life insurance agreement or an agreement 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, which implements Article 9(2)(a), GDPR).

The prohibitions in this Article only apply when both:

- The data subject executing the life insurance agreement or agreement with an endowment clause is in Croatia.
- The data controller is established in Croatia or provides services in Croatia.

(Article 20(3), Croatian Act.)

#### 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.

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

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

Public-sector entities may only process biometric data when both:

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

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

Public-sector data controllers do not need explicit data subject consent when the processing of biometric data 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, which implements 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:

- Carried out under the control of official authority (for example, the police).
- Authorized by EU or member state law providing for appropriate safeguards for data subjects.

(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 data controller implements appropriate safeguards. (Article 33, Croatian Act, which implements 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). In the absence of data subject consent, the secondary processing purpose must be compatible with the original processing purpose. To determine the secondary processing purpose's compatibility, the data controller should consider the criteria specified in GDPR Article 6(4).

## CHILD CONSENT

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 years old (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 years old (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 the Republic of Croatia (Article 19(2), Croatian Act). A violation of Article 19 of the Croatian Act is a violation a GDPR Article 8 and is subject to sanctions under GDPR Article 83 (Article 19(3), Croatian Act).

## DATA SUBJECTS' RIGHTS

The GDPR grants data subjects several rights and imposes several obligations on data controllers relating to those rights in Articles 12 to 22 and 34 (see Practice Note, Data Subject Rights Under the GDPR (w-006-7553)). The GDPR permits EU member states to restrict the scope of data subjects' rights and data controllers' related obligations found in these Articles when the restriction is a necessary and proportionate measure to safeguard certain objectives (Article 23, GDPR) (see GDPR Article 23 Objectives that Permit Restrictions to Data Subject Rights).

### GDPR ARTICLE 23 OBJECTIVES THAT PERMIT RESTRICTIONS TO DATA SUBJECT RIGHTS

EU member states may restrict the scope of data subjects' rights and data controllers' related obligations found in GDPR Articles 12 to 22 and 34 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 public interests of the EU or member state, in particular economic or financial interests, including monetary, budgetary and taxation, public health, and social security.
- Protection of judicial independence and judicial proceedings.
- The prevention, investigation, detection, and prosecution of breaches of ethics 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, prevention of crime, or breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing matters of civil law.

(Article 23(1), GDPR.)

When the data controller restricts data subjects' rights or limits its own obligations to ensure the GDPR Article 23 objectives, the data controller must consider, as appropriate, at least:

- The purposes of the processing or categories of processing.
- The categories of personal data.
- The scope of the restrictions.
- The safeguards to prevent abuse or unlawful access or transfer.
- The specification of the controller or categories of controllers.
- The retention periods and the applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- The risks to the rights and freedoms of data subjects.
- The right of data subjects to be informed about the restriction, unless doing so is prejudicial to the purpose of the restriction.

(Article 23(2), GDPR.)

### CROATIAN ACT VARIATIONS TO DATA SUBJECT RIGHTS

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

## DEROGATIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

The GDPR provides additional rules that apply to seven specific processing situations (Articles 85 to 91). These Articles permit EU

member states to enact further rules that apply to the specified types of processing. The Croatian Act introduces further rules that apply to:

- Processing for scientific or historical research and for statistical purposes (see Processing for Scientific or Historical Research and for Statistical Purposes).
- Secrecy obligations (see Secrecy Obligations).
- Processing in the employment context (see Processing in the Employment Context).

### PROCESSING FOR SCIENTIFIC OR HISTORICAL RESEARCH AND FOR STATISTICAL PURPOSES

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

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

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

These restrictions of data subjects' rights should be limited to situations where restricting data subjects' rights is strictly necessary to achieve the official statistical purpose and permitting data subjects to exercise their rights may hinder or impede achievement of the purpose (Article 33(1), Croatian Act).

Under the Croatian Act, data controllers are not required to notify data subjects about transfers of personal data for statistical purposes to the authorities competent for official statistics (Article 33(3), Croatian Act).

Personal data processed for statistical purposes must not allow identification of data subjects (Article 33(5), Croatian Act). Personal data processed for statistical purposes is also deemed compatible with the original collection purpose (see Processing for Secondary Purposes).

### SECRECY OBLIGATIONS

EU member states may adopt rules specifying the powers of supervisory authorities with respect to data controllers and data processors that are subject to an obligation of professional secrecy or other equivalent secrecy obligation (Article 90, GDPR). The Croatian Act states that any processing of information classified as secret under a special law must be conducted in accordance with that law (Article 39(1), Croatian Act, which implements GDPR Article 90). Only officials holding a valid certificate required to access classified information can access, copy, or otherwise process information classified as secret under special laws (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).
- The use of 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. Other laws' requirements are generally 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.

### 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 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 of employees' IDs. Employees may choose between biometric processing for these purposes or the other solution offered.

(Article 23, Croatian Act, which implements Article 88, GDPR).

Data controllers must obtain employee consent before processing biometric data (Article 23, Croatian Act).

### WORKPLACE SURVEILLANCE

The Croatian Act permits employers to use video surveillance in the workplace if the employer satisfies the Croatian Act's general requirements for lawful use of video surveillance and the requirements for video surveillance in the Occupational Safety Act. For more, see Video Surveillance.

## OTHER GDPR DEROGATIONS

### SUPERVISORY AUTHORITY

Croatian Act Article 4 establishes the Croatian Data Protection Authority (Croatian DPA) as required by GDPR Article 54. In addition to the powers specified in GDPR Article 58, the Croatian DPA has additional powers specified in the Croatian Act, including powers to:

- When prescribed by special laws, initiate and participate in criminal, misdemeanor, administrative, and other judicial and non-judicial proceedings for GDPR and Croatian Act violations.
- 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 the 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 Police Directive (Directive 2016/680), unless prescribed differently by special laws.
- Perform other tasks mandated by law.

(Article 6, Croatian Act, which implements Article 58(6), GDPR.)

## ADMINISTRATIVE FINES

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

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

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

- Violations of Croatian Act Article 27, which requires the data controller or data processor to provide information on video surveillance.
- Violations of Croatian Act Article 28, which requires the data controller or data processor 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 purpose of collection.

(Article 51, Croatian Act.)

For more on enforcement and sanctions under the GDPR, see Practice Note, GDPR and DPA 2018: enforcement, sanctions and remedies (UK) (w-005-2487).

### 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 a data subject to mandate one of these organizations to lodge a complaint with a supervisory authority on the data subject's behalf, if the organization:

- Is formed in accordance with 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 mandated by a data subject, such organizations may exercise the data subject's rights to:

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

(Article 41, Croatian Act, which implements 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 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 data controller's official authority under GDPR Article 6(1)(e).

(Article 6(2), GDPR.)

When using video surveillance, the Croatian Act requires that:

- The data controller only processes personal data collected through video surveillance for a purpose that is necessary and justified to protect individuals and assets and provided data subjects' interests do not override the need for data processing through video surveillance (Article 26(1), Croatian Act).
- The data controller, data processor, or other persons authorized by them do not use the personal data for any purpose different from the lawful purpose for which it was collected (Article 28(2), Croatian Act).
- The data controller or data 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 or public transportation vehicles, the surveillance of which is necessary to protect individuals and assets (Article 26(2), Croatian Act).
- The data controller or data processor provide data subjects with the information required by GDPR Article 13 (Information to be provided where personal data are collected 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 data controller; and
  - contact details for data subjects to exercise their rights relating to their personal data.

  (Article 27, Croatian Act.)
- Only the data controller, data processor, or other persons authorized by them access video recordings and the data controller or data processor must implement security measures to protect the video surveillance system from unauthorized use (Article 28, Croatian Act).

- The data controller and data processor 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). Only the data controller, data 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(5), Croatian Act).
- The data controller or data 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.)

Employers conducting workplace video surveillance must also comply with the Occupational Safety Act, which requires the data controller or data processor to:

- Refrain from installing video cameras in private areas, such as bathrooms or dressing rooms.
- Adequately inform employees 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 movements of employees or the employers are under surveillance the entire working time.

(Article 43, Occupational Safety Act, in relation to Article 30, Croatian 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 and public areas in Articles 31 and 32. The Croatian Act 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 assets.

(Article 32, Croatian Act.)

Data controllers using video surveillance in public areas must still carry out a data protection impact assessment if the data controller satisfies the conditions under GDPR Article 35 (Article 32, Croatian Act; see Practice Note, Data protection impact assessments under the GDPR (w-012-3168)).

## CROATIAN ACT AND GDPR STATUTORY REFERENCES

| Subject Matter | 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(1) | |
| Appointing a data protection officer (see Data Protection Officers) | NA | 38(5) |
| Requirements for processing special categories of personal data (see Processing Special Categories of Personal Data) | See Genetic, Biometric, and Health Data | 9(1) and 9(2)(b), (g), (h), (i), (j), 89(2) |
| 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) | NA | 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 Scientific or Historical Research and for Statistical Purposes | 23 |
| Processing for scientific or historical research and for statistical purposes (See Processing for Scientific or Historical Research and 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) |

| Subject Matter | Act Article | GDPR Article(s) Permitting Member State Derogation |
|---|---|---|
| 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) |



*02-19*