ZAGREBAČKI HOLDING

ZGH-01-18-359
01-01-02-18-04

# PERSONAL DATA MANAGEMENT SYSTEM POLICY OF ZAGREBAČKI HOLDING D.O.O.

■ ZAGREBAČKI HOLDING d.o.o.
Zagreb, Ulica grada Vukovara 41
Phone + 385 1 6420 000
www.zgh.hr

■ Commercial Court in Zagreb, registration number: 060042653
PIN: 85584865987
Zagrebačka banka d.d., Zagreb
IBAN: HR66 2360000-1101360753

# Content

# 1. Subject

With this Policy, the Management Board of Zagreb Holding d.o.o. provides full support for the personal data management system. The personal data management system must be fully compliant with the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The objective of personal data protection is to protect the private life and other human rights and fundamental freedoms in the collection, processing, and use of personal data. Personal data is any information relating to a natural person (data subject) who is identified or can be identified. This data must be handled with special care and this process shall be guided by the highest ethical principles. Work must be done to raise awareness that personal data is a very valuable and confidential asset. It is necessary to develop and implement a program to build a corporate culture of personal data confidentiality.

# 2. Reference documents

- Regulation (EU) 2016/679

# 3. Collection and processing

The collection and processing of personal data is only permitted if there is a legal obligation or an obligation based on a contractual relationship, while all other processing of personal data is only permitted with the express consent of the owner or his authorized representatives. The data must be accurate, complete and proportionate to the purpose for which they are processed. When personal data is collected, the data subject shall be informed of his/her identity and contact details, the purposes of the processing and the legal basis for the data processing, the recipients, the transfer to third countries, the storage period and the possibility of withdrawing consent. The collection of personal data from children is approached with particular care and must be guided by the highest ethical principles.

# 4. Rights of data subjects

- It is necessary to provide the data subject with all information related to the processing in a concise, transparent, understandable, and easily accessible form.
- The data subject has the right to view the personal data that are in the data collections and that relate to him/her.
- The data subject has the right to obtain the correction of incorrect personal data relating to him/her.
- The data subject has the right to request the deletion of personal data relating to him/her and for which he/she has given his consent.
- The data subject has the right to withdraw the given consent for the processing of personal data and request the termination of the processing of personal data.
- The data subject has the right to receive personal data relating to him/her, which he/she provided to the data controller in a structured, commonly used and machine-readable format.

# 5. Record of personal data processing

Zagrebački holding d.o.o. will create a central register of all collections of personal data. A responsible person must be designated for each collection. The processing collection must include the identity of the controller with contact information, the purpose of the processing, a description of the data subjects and personal data, the recipients of the data, information about the transfer of data to third countries and the expected data retention periods.

# 6. Data protection

Zagrebački holding d.o.o. will take all necessary technical, administrative and physical personal data protection measures in order to protect data from unauthorized access and possible misuse. When building new information systems, the requirements of the GDPR for the protection of personal data must be taken into account from the very beginning and their implementation must be ensured.

# 7. Incident management

Zagrebački holding d.o.o. will establish and maintain:

- response plan to incidents related to the breach of the security of personal data.
- register of incidents of breach of personal data security.
- the process for notifying the supervisory authority and the person that damage with regard to data was caused to about incidents of personal data security breaches.

In the event of a breach of security of personal data, it is necessary to report it to the competent authority without undue delay, but no later than 72 hours after the discovery of the incident. In the event of personal data becoming known, the owners whose data has been compromised must be informed of the personal data breach in clear and simple language.

# 8. Certification

Zagrebački holding d.o.o. will implement and maintain the applicable standards in the field of data protection and information security ISO 27001 with its personal data management system and will demonstrate compliance through appropriate certification, when possible.

# 9. Exceptions

Where there are legitimate grounds, the personal data protection officer may authorize the temporary processing of personal data that is not in compliance with this Policy. The data protection officer is obliged to keep records of such authorizations, responsibilities and deadlines for harmonization and report them to the Management Board.

# 10. Responsibilities

- All employees of Zagrebački holding d.o.o. must comply with the measures set forth in this Policy, as well as third parties who gain access to personal data in the course of their cooperation with Zagrebački holding d.o.o.
- The personal data protection officer is appointed by the Management Board and he is responsible for his work directly to the Management Board. The personal data protection officer is responsible for the establishment and maintenance of the personal data management system and the coordination of all activities related to personal data management. The personal data protection officer is responsible for:
    - informing and advising the controller or processor, as well as employees who process personal data about their obligations under the Regulation,
    - monitoring compliance with the Regulation and internal policies and other regulations related to the protection of personal data,
    - establishment and maintenance of a register of personal data,
    - assignment of responsibility for the protection of personal data to employees and third parties involved in the collection and processing of personal data,
    - raising awareness and education in the field of personal data protection,
    - incorporating privacy protection into business processes and information systems,
    - incorporating privacy protection into audit processes,
    - consulting in the implementation of data protection impact assessments,
    - cooperation with supervisory bodies,
    - supervision of the risk management process in the processing of personal data
    - reporting to the Management Board on the effectiveness of the personal information management system.
- The organizational unit responsible for IT is responsible for operationally establishing and maintaining the technical controls necessary to comply with the requirements of this Policy, and in particular for the measures taken to protect personal data and meet the requests of the owners of personal data.
- The head of IT security is in charge of the monitoring of the personal data security measures implementation and providing professional support in their field, as well as the operation of the personal data management system.

- The organizational unit responsible for legal affairs is responsible for monitoring and interpreting data protection regulations and providing legal support for the operation of the personal data management system.
- Internal auditing is responsible for the auditing of the operation of the personal dana management system.

This Policy is reviewed at least once a year or after any change in the legal or risk environment that could have an effect on its effectiveness.

The personal data protection officer is responsible for maintaining this Policy.

## 11. Entry into force and application

This Policy enters into force on the day of its adoption by the Company's Management Board and binds the Company as a whole as well as all its organizational units.

CHAIRWOMAN OF THE MANAGEMENT BOARD
Ana Stojić Deban
*Signed*

*Stamp:*
*ZAGREBAČKI HOLDING*
*d.o.o.*
*ZAGREB, Ulica grada Vukovara 41*