

## PERSONAL DATA PRIVACY POLICY

This Personal Data Privacy Policy (hereinafter: Privacy Policy) specifies details of the ways in which CRH (Serbia) doo (hereinafter: the Company) is processing personal data of its employees or the people cooperating with the company.

This Policy was set up in compliance with the Law on Personal Data Protection ("Official Gazette RS, no. 87/2018) (LPDP) which is coming into effect as of 21.08.2019 and applicable subordinate legislation, as well as with the General Data Protection Regulation EU 2016/679 (GDPR), which shall be significant in cases when its application is expected.

In this respect, CRH (Serbia) doo as a member of the CRH Group, with a registered office within the EU, has adopted these guidelines to the full.

The terms written in bold used in the Privacy Policy have been defined in the Glossary in Addendum I.

### CONTENTS

1 Scope.....	2
2 Purpose.....	2
3 Types of Personal Data.....	2
4 Purpose of Data Processing.....	3
5 Profiling.....	3
6 Individuals Rights.....	3
7 Security.....	6
8 Personal Data Disclosure .....	6
9 Personal Data Retention.....	6
10 Transfer of Data out of Serbia.....	6
11 Roles and Responsibilities.....	6
12 Procedure of Filing a Complaint.....	7
13 Related Policies.....	7

## **1.SCOPE**

This Privacy Policy applies to all personal data we, as a Data Controller, process.

The Company is a Data Controller of the Personal Data which is processed for the purposes and in the manner the Company determines.

The Company, for instance, can process personal data of its employees, former employees, their family members, temporary employees, self-employed persons, job applicants, contractors, suppliers' contacts, clients and visitors.

## **2.PURPOSE**

The purpose of this policy is to explain which personal data we process and why and how we do that. Besides, this Privacy Policy states our responsibilities and obligations related to protection of these data.

This Privacy Policy should not be understood as a complete statement about our practice relating to data protection, thus we shall inform you about variations, to the extent feasible.

## **TYPES OF PERSONAL DATA**

### **3.1 Employees and contractors**

The Company collects and processes personal data of our employees, job applicants and contractors, and former employees and contractors as well. This type of personal data includes: personal information such as name, date of birth, personal identification number, bank account information, relatives, information on social media accounts, information on visas/passports; contact information such as address and phone numbers; information from the employee's file such as employment terms and provisions, trainings, performance assessment, promotions, personal development plans, information on employee's behaviour and discipline, workplace location, salary, bank account, personal identification number, public personal identification number, security permits; employment history/information stated in the application such as education and employment history; editorial or newspaper content such as links to the papers, e.g. links to video or audio data files; medical information such as health certificates and sick leave certificates; information on family such as children's names and dates of birth (e.g. relevant if an individual requires parental leave); information required for retirement; information on syndicate membership and information relating to performance such as assessments obtained in the performance management process for managers and regular annual salary audits, psychometric tests, etc. The above mentioned list is not definite. It includes the personal data which is most frequently collected, used or processed in other ways.

### **3.2 Suppliers and Clients**

The Company collects and processes personal data of individuals who are our suppliers and clients and/or those cooperating with them. This personal data includes: personal information such as name, surname, personal identification number, identity card number, title, job, identification numbers in the company, department, operating unit (including contact information which is collected for training/verification): contact information such as e-mail address, phone numbers and workplace location.

### **3.3 Special categories of personal data**

Special categories of personal data a Company can process in special cases include, in compliance with the provisions of the Law on Special Categories of Personal Data, without limitations: data revealing racial or ethnical origin, political opinion, religious or philosophical beliefs or syndicate membership, as well as processing of genetic data, biometric data for personal identification based on facial recognition (e.g. photos of a face generated by video surveillance footage), medical history, i.e. data on health condition such as health certificates and sick leave notification, data on sexual life or sexual orientation of an individual.

### **PURPOSE OF DATA PROCESSING**

The Company processes personal data for purposes the personal data has been collected for.

Common reasons for personal data processing are: payroll and benefits administration; HR, performance and talent pool management; marketing and PR; improvement of company products and services; research and statistical analysis; business strategy; internal supervision or investigation; prevention and detection of unlawful and/or criminal behaviour intended against us or our clients and employees and/or fulfilling legal obligations. Occasionally, we can process personal data for other reasons. The Company is trying to inform its clients about the purposes of data processing once their consent have been acquired. If it is not possible or feasible, the company tries to provide you with information at short notice after data processing. Individuals have the right to withdraw their consent at any time.

### **Profiling**

The Company can process personal data of different individuals (e.g. employees, contractors and job applicants) so as to manage talent-pool and assess workforce (in order to potentially include the job attendance and performance analysis).

The individual whose personal data are processed has the right to be excluded from application of the decision based solely on automated processing, which includes profiling, if this decision results in legal consequences affecting this individual or if this decision significantly affects him/her, except for the cases when this decision is : (i) necessary for conclusion or execution of the contract between individuals the data refer to and the Data Controller; (ii) legally founded, if this law prescribes appropriate measures for protection of rights, freedoms and legitimate interests of individuals to which the data relates; (iii) based on the explicit consent of the individual to which the data relates.

### **INDIVIDUAL RIGHTS**

Individuals have certain rights based on Personal Data Protection Regulation.

**6.1 Right to be informed:** you can demand from us the information related to: (i) identity and contact data of the Data Controller, as well as of its representative, if it has been appointed; (ii) the contact data of the Data Protection Officer (if available); (iii) the processing purposes and legal basis; (iv) any legitimate interests pursued by the Data Controller, if the processing is conducted pursuant to Article 12, paragraph 1, item b of the Law on Personal Data Protection; (v) the recipient or group of recipients of personal data if they exist (vi) the fact that the Data Controller has any intention to transfer the data to another country or international organization, and if the country or the

international organization on the list of countries/international organizations with appropriate level of protection and directing to appropriate measures of protection, and how the data subject can be informed about these measures in case of transfer from Article 65 of the Law on Personal Data Protection (transfer with application of appropriate protective measures) and Article 67 (compulsory business regulations) or Article 69, paragraph 2 (in case the transfer is necessary for execution of a contract between the data subject and the Data Controller or for the application of precontractual measures undertaken upon the request of the data subject), as well as about the directing to appropriate protective measures, and the manner the data subject can be informed about these measures.

When collecting personal data, the Data Collector is obliged to provide the data subjects with the information referring to the following : (i) the data retention period, or if this is not possible, the criteria for determining this period; (ii) the right to request access from the Data Controller, correction or erasure of their personal data, or the right to restrict processing, the right to complaint and the right to data transfer; (iii) the right to revoke consent at any time, and the withdrawal of consent does not influence the permission to process based on consent before the withdrawal in case the processing is conducted based on the explicit consent of the data subject (Article 12, paragraph 2, item 1 of the Law on Personal Data Protection); (iv) the right to file a complaint to the Data Protection Officer; (v) if provision of personal data is a legal or contractual obligation or if provision of data a necessary condition for conclusion of a contract, and if the data subject has the obligation to provide personal data and what are the possible consequences in case the data is not provided and (vi) the automated decision-making, including profiling from Article 38, paragraphs 1 and 4 of the Law on Personal Data Protection, and least in those cases, appropriate information considering logic used in these situations, and the importance and expected consequences the processing has for the data subject.

If the Data Controller intends to process the personal data further, for another than intended purpose, the Data Controller is obliged to provide the data subject, prior to such processing, with the information relating to that purpose as well as to the above mentioned information.

If the data subject has already been informed about any of the above mentioned information, the Data Controller does not have any obligation to provide such information.

**6.2 Right to access:** you can request from us to provide you with a copy of your personal data processed by us or on our behalf. If a copy is requested by e-mail, the information is provided in a common e-form, unless the data subject had requested this to be done in a different form.

**6.3 Right to rectification and addition:** if you believe your personal data is incorrect or incomplete, you have the right to request your personal data to be rectified. Depending on the processing purpose, you have the right to complete your personal data, which requires providing an additional statement.

**6.4 Right to erasure:** you can request your personal data to be erased if : (i) it is no longer necessary for the intended purpose or another type of processing; (ii) if your consent to the processing has been revoked, in compliance with the Article 12, paragraph 1, item 1) or Article 17, paragraph 2, item

1) of the Law on Personal Data Protection, and there is no other legal basis for processing; (iii) if you have filed a complaint concerning processing in compliance with the Article 37 of the Law on Personal Data Protection; (iv) your personal data protection has been processed in an illegitimate manner; (v) if the personal data has to be erased so that the Data Controller can fulfill its legal obligations; (vi) if the personal data has been collected in connection with the usage of information services from Article 16, paragraph 1 of the Law on Protection of Personal Data.

**6.5 Right to restriction:** you can request from us to restrict processing of your personal data (i) if its validity is questioned, (ii) if our processing is illegal, and you oppose erasure of your personal data and request instead restriction of personal data, (iii) if you believe that we do not need your personal data any longer or (iv) if you have filed a complaint referring the processing and at the moment it is being estimated if the legal basis for processing by the Data Controller outweighs personal interests for implementing restriction.

**6.6 Right to data portability:** the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, the processing is based on consent of the data subject and if the data processing is automated. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

**6.7 Right to lodge a complaint:** a data subject has the right to lodge a complaint concerning processing of his or her personal data based on legitimate reasons for processing, conducted pursuant to Article 12, paragraph 1, item 5) processing is necessary in order to do business in public interest or exercising legally binding authorization of the Data Controller and 6) processing is necessary in order to exercise legitimate interest of the Data Controller or the third party, unless these interests have been outweighed by interests or basic rules and freedoms of the data subject requesting protection of personal data, especially if the data subject is a minor, including profiling, based on the above mentioned regulations. Data Controller is obliged to stop processing of the personal data of the data subject who has lodged a complaint, unless it has warned that legitimate reasons for processing outweighs personal interests of the data subject (see the Processing Purpose Section above).

#### **6.8 Automated decision-making:**

The Procedures on individual rights of the company provide explanations on exercising the above mentioned rights and how the company will manage them.

## **SECURITY**

### **7.1 Security measures**

The Company has put in place technical and organizational measures for protecting personal data from unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access. Personal data are kept safe with the help of numerous security measures including, where applicable, physical measures such as locked file cabinets and various IT measures.

Additional information relating to security measures can be found in the section Information Security Policy.

## **7.2 Personal Data Breach**

The Company shall manage personal data breach in compliance with the reporting procedure in case of a personal data breach. You can find the instructions on how to identify and report a personal data breach in our Personal Data Breach Procedure.

## **DISCLOSURE OF PERSONAL DATA**

Occasionally, the Company can disclose personal data to third parties or allow third parties to access the personal data we are processing (e.g. if the legal department or a regulatory body file a valid request for access to personal data).

Any disclosure of personal data to third parties or granting permission to third parties to access shall be conducted in compliance with the Law on Personal Data Protection, based on the data subject consent or without the consent, in compliance with Article 12 of the Law on Personal Data Protection, in cases when consent is not legally prescribed.

The Company can share personal data with; (a) other members of the CRH Group (including our subsidiaries, holding company and its subsidiaries); (b) with selected third parties including business partners, suppliers and subcontractors; (c) with third parties in the process of buying or selling a company or property or (d) if the company has a legal obligation to disclose personal data. This includes exchange of information with other companies and organizations for the purpose of fraud prevention.

If the Company enters into a Data Processing Agreement with third parties who shall process data on our behalf or if execution of the Agreement, besides the defined subject, includes personal data processing as well, it will ensure that appropriate contractual obligations protecting this data are in place. This, for instance, includes providers of communication services, payroll services and providers of other services from the area of Human Resources, OHS services, advertising agencies or employment agencies, data centre operators, etc.

## **DATA RETENTION**

The Company keeps personal data for as long as the retention of this data is considered to be necessary for the purposes the personal data is being processed for. Personal data is retained in compliance with relevant laws and bylaws, as well as with relevant general acts and company policies.

## **TRANSFER OF DATA OUT OF THE TERRITORY OF SERBIA**

From time to time, the Company might have to transfer data out of the territory of Serbia. This transfer shall be carried out in compliance with applicable regulations relating to data protection. The Company undertakes reasonable steps so as to ensure the personal data are dealt with in a responsible manner and in compliance with the Law on Personal Data Protection and this Privacy Policy when transferred out of the territory of Serbia.

## **ROLES AND RESPONSIBILITIES**

The Company is responsible for personal data processing. The Company MD bears the general responsibility for the company compliance with this Privacy Policy and shall delegate a primary contact person in relation to (i) processing of personal data relating to current and former employees and company contractors; (ii) processing of personal data relating to business contacts and (iii) protection of security and integrity of personal data processed by the Company.

Legal Department shall support the Company by providing legal advice and instructions when interpreting regulations on data protection and this Data Protection Policy locally.

All employees in the company have to comply with the latest version of the Privacy Policy, which shall be published from time to time. If it is found out that employees have intentionally breached this policy, they shall be subject to disciplinary procedures, even to the possibility of being fired in compliance with internal rules regulating rights and obligations of employees.

## **PROCEDURE OF LODGING A COMPLAINT**

You can ask questions relating to this Privacy Policy and/or processing of your personal data or to lodge a complaint about them by contacting the HR Department or the Legal Department.

Although you can lodge a complaint to a relevant data protection regulator in relation to our compliance with data protection regulations, we insist that you first contact us by writing to the following e-mail address [ivana.boskovic@rs.crh.com](mailto:ivana.boskovic@rs.crh.com) so as to enable us to resolve your doubts, if you have any.

In Popovac, on 15.08.2019

CRH (Serbia) doo  
Milan Ilić  
Executive Director

Maja Stojiljković  
Executive Director

## ADDENDUM I

### GLOSSARY

The Privacy Policy is using the terms which have the following meaning:

**CCM** – Company Compliance Manager

**Data Controller** – is the entity which decides upon the purpose and means for the data processing.

**Personal Data** – is any information relating to a living person whose identity is defined or definable, directly or indirectly, especially according to identifiers, such as name and identification number, location, electronic communication network identifiers or one, or more identifiers of his/her physical, physiological, genetic, mental, economic, cultural and social identity. Personal data might include:

#### **Empoyees and contractors**

1. Personal information such as name, date of birth, bank account numbers, relatives, social media accounts.
2. Contact information such as addresses and phone numbers
3. Information from the employee's file including, for instance, employment terms and provisions, trainings, performance assessment, promotions, personal development plans, information on employee's behaviour and discipline, workplace location, salary, bank account numbers, personal identification number, numbers enabling personal identification, such as public personal identification number.
4. Employment history/information stated in the job application such as education and employment history
5. Editorial or newspaper content such as links to the papers, e.g. links to video or audio data files
6. Medical information, in special cases, in compliance with the provision of Article 17 LPDP on processing of special categories of personal data, such as health certificates and sick leave certificates
7. Information on family such as children's names and date of births (e.g. relevant if an individual requires parental leave)
8. Information required for retirement
9. Information on syndicate membership, in special cases, , in compliance with the provision of Article 17 LPDP on processing of special categories of personal data and
10. Information relating to performance such as assessments obtained in the performance managment process for managers and regular annual salary audits, psychometric tests, etc.

#### **Suppliers and clients**

1. Personal information such as name, title, job, identification numbers in the company, department, operating unit
2. Contact information such as e-mails, phone numbers
3. Workplace location and



4. Tax information such as Tax Identification Number/Personal Identification Number

**“Processing”** means any action or a group of actions which are automated or non-automated and include personal data or groups of data, such as collecting, recording, classifying, grouping, structuring, storing, adjusting or altering, disclosing, having insight, using, disclosing by transfer or delivering, multiplying, spreading or making available in other ways, comparing, restricting, erasing or destroying. Processing can be carried out manually or by means of automated systems such as information technology systems. “Processing” and “process” shall be interpreted accordingly.

**“Processing beyond boundaries”** includes the following: (a) in case of subsidiaries in several countries when personal data is processed in several countries or (b) when, in spite of the fact the personal data is processed in only one country, this processing significantly affects (or is likely to significantly affect) data subjects in several countries.

**“Data Processor”** is the party processing personal data on behalf of the Controller (e.g. payroll service providers).

**“Personal Data Breach”** is a security breach which leads to accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to of personal data being transferred, stored or processed otherwise.

**“Profiling”** is any form of automated processing consisting of the use of specific personal aspects, relating to a certain individual in particular to analyse or predict aspects concerning that individual’s performance at work, his/her economic status, health, personal interests, reliability, behaviour, location or movements.

**“Special categories of personal data”** means personal data revealing any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophic beliefs or syndicate membership. Special categories of personal data also comprise processing of genetic data, biometric data (e.g. biometric fingerprint data and a digital photograph), medical data, sex life or sex orientation.

**“Data on criminal offences and convictions”** representS categories of personal data related to criminal convictions, punishable acts and safety measures. Processing can be conducted only with the consent of a data subject and only under supervision of a competent authority or, if processing is permitted by law, with application of appropriate special measures protecting rights and freedoms of data subjects to which the data relates to.