

## DATA SUBJECT RIGHTS AND REQUESTS RELATED TO DATA PROTECTION

Law on Personal Data Protection (Official Gazette, no. 87/2018) (LPDP) states a large number of individual rights related to their personal data (Rights of the Data Subject). According to it, individuals have the right to address requests for review, alteration, amendment, erasure, restriction or rectification of their personal data, as well as the right to lodge a complaint to the way the data is being processed as well as to automated decision-making.

The objective of this document is to: (1) explain the Rights of the Data Subject and (2) explain how the individual requests for exercising their rights (requests) should be dealt with in compliance with the LPDP or other applicable laws. The diagram in the Addendum to this document illustrates possible ways how these requests might be managed.

### 1. RIGHTS OF THE DATA SUBJECT

Individual rights under the LPDP include:

#### A. The Right to be Informed

CRH, as a Data Controller, has the obligation to provide the data subject with the information, at the moment the data is being collected, related to: (i) identity and contact details 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 on that basis; (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)

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 from the Data Controller access, 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, LPDP) or based on the data subject consent to processing special categories of personal data (Article 17, paragraph 2, item 1, LPDP); (iv) the right to file a complaint to the Data Protection Officer; (v) if provision of personal data is legal or contractual obligation or if provision of data is 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 LPDP, 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 another 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

#### **B. The Right to Access**

CRH (Serbia) doo Popovac (the Company), as a Data Controller, upon the receipt of a request filed by a data subject, has the obligation to:

- confirm whether the personal data of the individual data subject is being processed
- to explain why and how the data is being processed and provide the individual with other information in relation to the personal data processing pursuant to Article 26 LPDP, and
- provide the data subject with a copy of personal data. In case the request is submitted 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.

#### **C. The Right to Rectification and Updating**

A Data Subject has the right to request his/her personal data which is incorrect to be erased without further delay. Depending on the processing purpose, a Data Subject has the right to update his/her incorrect personal data, which requires providing an additional statement.

#### **D. The Right to Erasure**

A Data Subject can request erasure of his/her personal data 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) LPDP, and there is no other legal basis for processing; (iii) if you have filed a complaint concerning processing in compliance with the Article 37 LPDP; (iv) personal data 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 LPDP.

If the Company has shared personal data with a third party (e.g. with a Data Processor, such as a payroll service provider), it is obliged to inform the third party about the erasure or restriction of relevant personal data.

## **E. The Right to Restrict Processing**

A Data Subject can request from the Company to restrict processing of his/her personal data (i) if its validity is questioned, (ii) if the processing is illegal, and the Data Subject is opposed to erasure of the personal data and requests instead restriction of personal data, (iii) if a Data Controller does not need the personal data any longer for the intended purposes or if a Data Subject requested them in order to submit, exercise or defend a legal claim; and (iv) if a Data Subject has 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.

When the processing is restricted, the Company is allowed to store the personal data, without further processing, unless or until this issue is resolved. Similarly, if the Company has shared personal data with a third party (e.g. with a Data Processor such as payroll calculation service provider), the Company has to inform the third party about the restriction of personal data processing imposed by the relevant individual until further notice. The third party has to be informed when this restriction is withdrawn.

## **F. The Right to Lodge a Complaint and Automated Decision-making**

Individuals have the right to lodge a complaint related to processing of their personal data, on account of reasons referring to their specific situation. In this case, the Company has to suspend processing of personal data, except for cases when irreversible legitimate reasons for processing can be proved (which shall be determined separately for each case).

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 rights and freedoms of the data subject requesting protection of personal data, especially if the data subject is a minor, including profiling, based on the items 5) and 6) paragraph 1, Article 12 LPDP. Data Controller is obliged to stop processing of the personal data of the data subject who has lodged a complaint, unless it has pointed out that legitimate reasons for processing outweighs personal interests of the data subject.

However, a Data Subject can lodge a complaint at any time, without an explanation, if the Company conducts processing for direct advertising purposes.

A Data Subject has the right to be excluded from implementation of decisions made based on automated processing (including profiling), which can result in legal consequences, i.e. have a significant influence on the Data Subject except for some specific cases. Examples of automated processing include decisions on loans made based on online information.

## **G. Data Portability**

If data subjects submit their personal data to a Company, they shall have the right to file a request:

- to receive the personal data in a structured, commonly used and machine-readable format and have the right to transmit the data to another controller without hindrance from the controller to which the personal data has been provided, the processing is based on consent of the data subject and if the data processing is automated and/or
- upon the request of a data subject the personal data to be transmitted directly from one controller to another, where technically feasible.

## **2. HOW TO MANAGE DATA SUBJECT REQUESTS**

### **A. Responding to a request**

The Company has to communicate with an individual who sent the request, or with a third party who the personal data is shared with, after the alteration, erasing or restriction.

Information or messages sent to individuals in a response to their request has to be:

- concise, transparent, intelligible and easily accessible, written in a plain language
- in writing (e.g. letter or e-mail) and if a data subject has such request, the information can be provided orally, on condition that the identity of a data subject has been unquestionably confirmed and
- individual requests made electronically (e.g. e-mail), should have the information provided in the same electronic format, (i.e. e-mail) if possible, unless the individual requires otherwise.

### **B. Deadline for Responding to Data Subject Requests**

After the receipt of a valid request, a reply has to be provided “without undue delay”, 30 days at the latest after the receipt of a request. That deadline can be extended for 60 days if necessary, depending on the complexity and number of requests. The Company has to inform the individual about the possible deadline extension within a month after the receipt of the request, as well as about the reasons for delay/extension.

If the Company has a valid and legitimate reason for not responding to a request within a prescribed time frame or not at all, it has to: (a) immediately inform the individual about the reasons for not undertaking any actions, in any case, within one month after the receipt of the request and (b) to inform the individual that he/she has the right to lodge a complaint with a competent Data Protection Authority or to file a lawsuit.

### **C. Costs of Responding to Requests**

All information/messages provided by the Company related to a request have to be free of charge unless the individual request is “evidently ungrounded or exaggerated”, especially if the request appears repeatedly (e.g. in case of sending the same request multiple times), when a Company can : (a) charge a reasonable fee to an individual (necessary administrative fees) or (b) reject a request. Providing evidence that the request was ungrounded or exaggerated shall be dealt with by the Data Controller.

**D. Any questions?**

In case you have any questions or need additional guidance, you can send your queries at [ivana.boskovic@rs.crh.com](mailto:ivana.boskovic@rs.crh.com). Furthermore, the Legal Department can advise you on interpretation of this procedure.

In Popovac, on 15.08.2019

CRH (Serbia) doo  
Milan Ilić  
Executive Director

Maja Stojiljković  
Executive Director

## ADDENDUM 1

### Managing Data Protection Requests – Diagram

If you have any questions or need further guidance, contact the HR Department or a (local) DPA. The Legal Department can advise you on interpretation of this procedure.

	Received request for:			
Access to personal data	Erasure or rectification of personal data	Restriction of personal data	Complaint to data usage	
Ask for a proof of identity	No	Are you certain about the applicant's identity?		
Ask the applicant for a clarification	No	Is the nature of the request clear? Find out where the relevant data is stored and ask the entire internal staff from the storage location to provide copies		
		Collect and check the relevant personal data in accordance with the request		
		Is the request very complex and/or is there a large number of requests which cannot be resolved within a month		
		No		
		Inform the applicant that their request shall be resolved with a delay (up to 2 months). Clarification shall include:		
		<ul style="list-style-type: none"><li>reasons for the delay</li><li>the right to file a complaint to a DPA</li></ul>		
Yes				
Access				
Think if there are any exceptions related to personal data disclosure				
Yes				
Erasure/rectification				
Think if there are exceptions preventing implementation of erasure /rectification requests				
Yes				
Restriction				
Think if it is possible to restrict personal data				
Yes				
Access				
Think if it is possible to lodge a complaint about personal data processing				
Yes				
Finalize the personal data which should be revealed to the applicant(make sure the data identifying other individuals has been removed)				
Yes				
Erasure/rectification				
Take into account and state all third parties you have shared the personal data with				
Yes				
Restriction				

Take into account and state all third parties you have shared the personal adata with

Yes

Access

Think if there are legal grounds binding you to continue data processing

Yes

Send the data and the response to the applicant-point out the deviations from the request, if there are some

Yes

Send the response to the applicant confirming the actions undertaken and, where feasible, state the reasons for inability to resolve the request or act accordingly.