PERSONAL DATA BREACH PROCEDURE

1. INTRODUCTION

The personal data breach procedure (hereinafter: the Procedure), gives a detailed account of the process of escalation, reporting and recording of an assumed or actual personal data breach incident involving personal data (as defined below), and it has been established in compliance with the Law on Personal Data Protection (Official Gazette no.87/2018) which came into effect as of 21.08.2018, with a reference to the General Data Protection Regulation, which can be applied to a company anticipated by the above mentioned regulation.

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

This Procedure refers to CRH (Serbia) doo Popovac (the Company).

The objective of this Procedure is to ensure that the company can manage a personal data breach incident (as defined below) and localize it fast so as to minimize the effects of the personal data breach and duly fulfill the obligation to report the breach to the Regulator and/or individuals affected by this breach.

2. WHAT EXACTLY IS PERSONAL DATA?

Personal Data is any information relating to a living person whose identity is defined or definable, directly or indirectly, especially according to identificators, such as name and identification number, location, electronic communication network identificators or one, or more identificators of his/her physical, physiological, genetic, mental, economic, cultural and social identity (personal data). A person can be identified if the identity can be reasonably ascertained based on the information without putting in much disproportionate effort. Personal data includes: the name, address, date of birth, telephone number, bank account number, job, photograph, IP address, etc.

3. WHAT IS A PERSONAL DATA BREACH

LPDP defines a personal data breach incident as a “security breach which can lead to accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data which is transferred, stored or processed in another way“ (personal data breach). Personal data breach examples are: loss or theft of a laptop or a mobile phone containing personal data; sending (unprotected) Excel files containing personal data to an unauthorized person; printing payroll information and leaving a printed copy in the printer; hacking the system containing personal data and/or loss or theft of data files, etc.

An incident including a personal data breach is described as “a data incident“. If a data incident does not include personal data, it shall not be considered as a data breach. However, not all data incidents involving personal data are considered to be personal data incidents. For instance, loss or threat to personal data might not be considered as a personal data breach in the following cases: (i) personal data is encoded or turned into anonymous data; (ii) there is a complete and updated personal data backup copy and (iii) access to

personal data is being supervised. In accordance with the above said, the decision to consider a data incident as a personal data breach incident shall be made respectively.

4. WHEN TO APPLY THE PROCEDURE?

If the data incident does not invlove personal data, this procedure shall not be applied. If the data incident involves personal data, it is likely that a personal data breach has occured and this procedure shall be applied. If there are any doubts whether a personal data breach has occured, the Company has to seek advice from the Legal Department immediately in order to get a quick assessment of the incident.

5. HOW CAN I REPORT A PERSONAL DATA BREACH INTERNALLY?

It is important to report immediately actual or presumed personal data breaches internally, within the CRH company, in compliance with the following steps:

5.1. First reporting

When a person becomes aware of an actual or presumed personal data breach, he/she should report it immediately to the CEO (Managing Director of the company) or directly to the Legal Department. The MD shall report any actual or presumed personal data breaches to the Legal Department.

5.2 Data Breach Response Plan

In case a personal data breach has occured, MD of the company or his delegate shall, in cooperation with the Legal Department, develop a personal data breach response plan. The Addendum A contains a diagram showing how a personal data breach incident should be managed.

When developing a relevant response plan, the team considering the incident takes the following into account:

- Information contained in the data breach notice
- Necessary actions which should be taken immediately so as to localize the security breach
- If there is a request to report the personal data breach to a relevant data protection authority –Comissioner for Information of Public Importance and personal data protection, and if there is one, what to report
- Potential consequences of the personal data breach which could affect the company and individuals
- Measures the company is undertaking and/or which it might take so as to minimize the damage inflicted to the individuals
- How shall the individuals be notified about the security breach, if appropriate in such circumstances, as well as the measures the individuals can take to alleviate further damage.
- If there is personal responsibility or responsibility of third parties due to personal data breach
- Inernal (or, where appropriate, external) communication and its timeline
- If, besides the Comissioner, other stakeholders should also be notified
- What can be learnt from the personal data security breach incident and what measures can be applied so as to prevent its recurrence.

5.3 Should a Comissioner be notified ?

It is not necessary to report every personal data breach to the Comissioner. The data Controller is obliged to inform the Comissioner in case the personal data breach can put rights and freedoms of individuals at risk. In other cases, reporting is not necessary.

If a personal data breach should be reported to the Comissioner, the Legal Department shall report the breach incident to the Comissioner after consultation with the company MD without unduly delay, or if possible, within 72 hours after the breach was reported. If the company does not report the breach within 72 hours after the reporting, it is obliged to provide explanation for not responding within this deadline.

5.4 Resolving

Having sent a notice to the Comissioner, and received the Comissioner's remarks, the Legal Department shall consult the company MD in order to manage the security breach and resolve it in compliance with the relevant personal data breach response plan.

6. WHAT TO REPORT TO A COMISSIONER?

The following should be reported to the Comissioner:

- Nature of the personal data breach, including relevant categories of personal data and approximate number of data subjects, and approximate amount of affected personal data.
- Name and contact details of a CRH contact person which can provide additional information related to personal data breach, or information concernig other ways of obtaining information about the breach;
- Possible consequences of the personal data breach
- Measures which have been taken or proposed by the Data Controller in order to resolve the security breach, including the measures undertaken in order to minimize harmful consequences;
- Measures which affected individuals can take in order to limit the harmful consequences of the personal data security breach.

7. PERSONAL DATA BREACH NOTICE TO AFFECTED INDIVIDUALS

An affected individual should be notified only if the personal data security breach can lead to a high level risk to the rights and freedoms of the data subject. Reporting the security breach to affected individuals shall be carried out in compliance with the relevant response plan. The notice sent to the affected individuals should contain at least: (i) name and contact details of a CRH contact person which can provide additional information concerning the personal data breach; (ii) information on the nature and extent of the personal data breach; (iii) desciption of established and assumed consequences which the personal data breach shall have on the personal data (iv) measures taken or measures that shall be taken by the Company in order to limit the negative consequences of the personal data breach, inculding the measures undertaken in order to minimize the harmful consequences;

A notice shall not be sent to individuals in the following cases: (a) the company has implemented appropriate technical, organizational and personnel measures due to which personal data is illegible to unauthorized persons, e.g. by means of encoding, crypto protection or other measures; (b) the company has subsequently taken measures which can prevent a high level risk personal data breaches, which could affect rights and freedoms of data subjects and (c) if sending a notice to data subjects would represent a disproportionate expense of time and resources, the Data Controller is obliged to inform the data subject by means of public information or in another efficient way.

8. REGISTER OF PERSONAL DATA BREACHES

A company must create and keep a register where all data security breaches shall be recorded. The Legal Department shall keep the register of personal data breaches and accordingly report them to the company (each is called “a register“).
The purpose of keeping a register of personal data breaches is : (i) to provide a lesson derived from the personal data breach and the way it was resolved; (ii) to provide, if necessary, concise answers to questions received from affected individuals and/or the Comissioner and (iii) to provide the Comissioner with a resume, if requested.

For each personal data breach, the following information shall be recorded:

- Date and exact time when a personal data breach was reported
- Name and contact information of affected individuals
- Facts and information on the nature of the personal data breach
- The person to whom the personal data breach has been reported and why and
- Actions taken after a personal data breach has been detected (such as personal data breach recurrence prevention measures, etc).

The company has to keep the register containing the list of personal data breaches reported to the Comissioner within the period of five years at least.

In Popovac, on 15.08.2019

Milan Ilić
Executive Director

Maja Stojiljković
Executive Director

ADDENDUM I

Process flow diagram in case of a personal data breach

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

Suspected Personal Data Breach Incident

Reporting — Report it to the company MD and Legal and Compliance Department

Assessment — Company MD and Legal and Compliance Department assess if the personal data breach has occured

If a Personal Data Breach has occured	If a Personal Data Breach has not occured
Response Plan Legal and Compliance Department, with the MD or a delegate, prepare a Response Plan	In this case, no further response is needed

Should a Comissioner be notified?

Legal and Compliance Department considers reporting to a Comissioner	If it is not necessary, the data breach register should be updated. Discuss the findings and further actions. In this case, no further actions are needed.

Notice to a Comissioner

If necessary, Legal and Compliance Department sends a notice to a Comissioner within 72 hours and notifies the stakeholders

Resolving and recording

The incident has been resolved.

Personal Data Breach Register has been updated.

Discuss the findings and necessary further actions.