Valitor rules for the handling of customer data

1. Purpose and scope

1.1 These rules are set by the Board of Valitor hf. (Also referred to as "the Company") with reference to Article 19. b Act on Financial Undertakings. 161/2002.

1.2 Valitor strives to ensure the privacy of its customers and that customer information is handled in accordance with the requirements of current legislation governing the use and security of information, requirements of the law on confidentiality of Bank Employees and the security regulations that the company has instituted. The aim of these rules is to inform customers of the Company on how this is done.

1.3 These requirements apply to all information held by the company concerning its customers, regardless of the form in which such information is retained. The regulations apply to Board members, directors, auditors, employees and any other persons who undertake work for the company.

2. Use of information

2.1 Valitor may store information that customers provide the company upon commencement of a business relationship and while the business relationship is maintained. Information that the company may receive from third parties, such as Creditinfo, may also be retained.

2.2 Storage of customer information shall done in accordance with the company's information security policies, applicable laws and standards that the company has undertaken to adhere to.

2.3 Valitor strives to ensure that customer information retained by the company is accurate and precise. False, misleading, incomplete and outdated information shall be corrected and, when applicable, deleted. Information about customers shall be destroyed when there is no longer a reasonable need to retain them.

3. Staff access to information

3.1 Information stored by the company is access-controlled. Employees only have access to information necessary for the conduct of their work.

3.2 The heads of departments and divisions provide users under their supervision access in accordance with levels prescribed by the Company’s information security policy. Regular reviews are carried out by the security manager to determine whether permissions are excessive.

Valitor // Dalshraun 3, 220 Hafnarfjörður // 525-2000 // valitor@valitor.is // www.valitor.is

3.3 Any access of sensitive information, such as cardholder information, shall be recorded and include an audit trail.

4. Confidentiality and disclosure to third parties

4.1 Valitor ensures that there is no unauthorized access to information about customers. For this purpose external access controls have been set up at Company facilities as well as technical access controls, such as firewalls, passwords and security system components to prevent unauthorized access of computer and communications systems.

4.2 Company employees are bound by confidentiality and all employees who handle personal information sign a separate agreement on confidentiality before being allowed access to such information. The obligation to maintain confidentiality continues even though employment has been terminated.

4.3 Customer information may only be released to third parties if there is a clear legal authority or with the written consent of that customer. In some cases the Company may be obliged to disclose information to a third party, e.g. on the basis of law no. 64/2006 concerning measures against money laundering and terrorist financing.

4.4 Official monitoring bodies, including. The Financial Supervisory Authority, The Competition Authority, tax authorities and police, have the legal right to request information about the company's customers and in such cases the company may be required to comply with such requests.

4.5 When supplying information to third parties, employees shall follow internal procedures and regulations, as applicable.

5. Rights of customers

5.1 The Company's customers are entitled to obtain from the Company, if requested, any information about that customer which the Company is using or has used, the purposes of processing the information, who has or will receive information about that customer, from where does this information come and what safeguards are in place with processing, provided it does not impair the security of data processing.

5.2 Requests for information under. Article 5.1 must be sent to the Compliance Officer of the Company] who arranges for the delivery of information.

5.3 The company shall comply with information requests as soon as possible, but no later than within 30 days of receipt of the request.

Valitor // Dalshraun 3, 220 Hafnarfjörður // 525-2000 // valitor@valitor.is // www.valitor.is

5.4 Access to information may be refused, in whole or in part, if the delivery is contrary to privacy considerations or statutory confidentiality requirements of the company.

6. Control and monitoring

The Board is responsible for the security of customer information and the daily management of information security is performed by the Security Manager

7. Publication and entry into force

7.1 These rules have been approved by the Board and take effect August 25, 2016.

7.2 These regulations shall be made available to customers and are published on the company website www.valitor.is.

Húsafelli 21. september 2016

_____
Guðmundur Þorbjörnsson, form.

_____
Synnöve Trygg, varaform.

_____
Jónína S. Lárusdóttir, meðstj.

_____
Roger Alexander, meðstj.

_____
Stefán Pétursson, meðstj.

Valitor // Dalshraun 3, 220 Hafnarfjörður // 525-2000 // valitor@valitor.is // www.valitor.is