

Definition of Terms:

Company – a member company of the Soci t  G n rale Group, specifically: ALD Automotive s.r.o., U Stavoservisu 527/1, 108 00 Praha 10, Czech Republic, I O/Company ID: 61063916 (**ALD**); ALD Automotive Slovakia s. r. o., Pan nska cesta 47, 851 04 Bratislava, Slovak Republic, I O/Company ID: 47 977 329 (**ALD SK**); ESSOX s.r.o.,  esk e Bud jovice, Senov zn  n m. 231/7, Postal Code: 37021, Czech Republic, I O/Company ID: 26764652 (**ESSOX**); Factoring KB, a.s., n m st  Junkov ch 2772/1, 155 00 Praha 5, Czech Republic, I O/Company ID: 25148290 (**FKB**); KB Penzijn  spole nost, a.s., n m st  Junkov ch 2772/1, Praha 5, Postal Code: 155 00, Czech Republic, I O/Company ID: 61860018 (**KBPS**); Komer n  banka, a.s., Na P ikop  33  p. 969, Praha 1, Postal Code: 114 07, Czech Republic, I O/Company ID: 45317054 (**KB**); Komer n  banka, a.s., pobo ka zahrani nej banky, Hod ovo n mestie 1A, Bratislava, Postal Code: 811 06, Slovak Republic, I O/Company ID: 47 231 564 (**KBSK**); Komer n  poji tovna, a.s., Praha 8, Karolinsk  1,  p. 650, Postal Code: 18600, Czech Republic, I O/Company ID: 63998017 (**KP**); Modr  pyramida stavebn  spo itelna, a.s., B lehradsk  128,  p.222, Praha 2, Postal Code: 12021, Czech Republic, I O/Company ID: 60192852, (**MPSS**); SG Equipment Finance Czech Republic s.r.o., n m st  Junkov ch 2772/1, Praha 5 – Stod lky, Postal Code: 155 00, Czech Republic, I O/Company ID: 61061344 (**SGEF**); SG Equipment Finance Czech Republic s.r.o. - organiza n  zlo ka, Hod ovo n m. 1A, Bratislava 1, Postal Code: 811 06, Slovak Republic, I O/Company ID: 31785972 (**SGEF SK**); STD2, s.r.o., V clavsk  n m st  796/42, Nov  M sto, 110 00 Praha 1, ID:27629317;VN 42, s.r.o., V clavsk  n m st  796/42, Nov  M sto, 110 00 Praha 1, ID: 02022818; KB SmartSolutions, s.r.o.,V clavsk  n m st  796/42, Nov  M sto, 110 00 Praha 1, ID:02021161.

Company's Responsible Employee – a senior manager with personnel authorities, i.e. an employee of the Company who is responsible for the delivery of the services provided to a defined extent through the agency of the External Employees.

Contracting Partner – an employer or a cooperating entity that, under a contractual relationship, provides the services to the Company through the agency of the External Employees.

External Employee – an employee of the Contracting Partner of any of the SoGe Group companies, which is a user of the IS and works, directly or indirectly, with confidential information concerning the company and its clients. For this reason, the External Employee shall be obliged to familiarise himself/herself with and adhere to the current safety policy of the Company and with internal regulations concerning the IS.

Information System (IS) is a working whole designed to collect, process, store and made accessible information in a purposeful and systematic manner. Technical means and devices (computers, IT technologies), software, information bases (databases), and working & organizational procedures used by member companies of the Soci t  G n rale (SoGe) Group are part of the IS.

The External Employee shall be obliged to observe the below rules and principles:

1. In terms of IS security, the External Employees shall be treated as the Company employees.
2. Each External Employee must have his/her **personal account in the DS domain**, i.e. shall have a personal number assigned, while the Contracting Partner shall assume **liability for a possible damage** caused by its Employee.
3. The IS tools and outputs can only be used in connection with activities that **fall within the scope of the contracted works** assigned to the External Employee under the contract entered into by and between the Company and the Contracting Partner, or based on **instructions issued by the Company's Responsible Employee**.
4. The External Employee may only use the information and data retrieved from the IS for the purpose of **executing the contracted works and hand them over to authorised individuals**¹. The information and data that should not be published outside the Company must be kept secret.
5. **Authorised means of access to the IS can only be used**. Trying to access the IS in an unauthorised manner, particularly by using other persons' access profiles and authorisations, and to break through current IS security measures is prohibited.
6. If the External Employee finds out that he/she is allowed **access also to other parts of the IS** than those associated with his/her job (in particular when his/her job description is changed), he/she must **immediately notify the Company's Responsible Employee**, who shall see to it that superfluous rights shall be revoked in accordance with the need-to-know principle and effective internal regulations.
7. The External Employee shall be obliged to **keep the information necessary for IS authentication and access to cryptographic keys** (e.g., a password or a PIN code) **secret, and not to disclose it to unauthorised individuals**; If such information is disclosed, or disclosure is suspected, it must be immediately altered (if possible) and the Company's Responsible Employee must be informed.
8. If the External Employee has received authentication tools to be used with systems and cryptographic keys (e.g., a chip card or a security box), he/she shall **not let another person use them** and must **keep them safe**. Any possible loss of such authentication tools must be reported to the Company's Responsible Employee.
9. The External Employee **must not use and disseminate suspicious and unverified information** and data delivered by electronic mail or stored on portable magnetic media (a CD, USB drive etc.).
10. Any unauthorised **tampering with the IS**, in particular installing software, setting/adjusting system parameters, and/or modifying the hardware **is strictly prohibited**. Such activities are reserved to employees authorised by the Company. Deleting and/or modifying data not directly related to the assigned job is also prohibited.
11. The External Employee shall be obliged to **adhere to the licensing policy**, particularly not to make the company software available to other entities.
12. The External Employee shall be obliged to report to the Company's Responsible Employee any information system errors and failures, **infringement of the IS security**, possible **risks and detected security threats and incidents** connected with the IS.

¹ An individual authorised to handle the information in accordance with the Company's information confidentiality categorizing model or, as the case may be, based on an authorisation or approval given by an owner of the information.

Duties of external specialists using the Information System

13. The External Employee shall be obliged to **keep the used IS tools safe from possible misuse** (in particular, log off the applications and the system; activate a security screensaver protected by a password when leaving the workstation; physically secure the hardware). The External Employee shall further be obliged **keep IS outputs** stored on portable media or in a printed form **in a safe place**.

Any breach of the aforesaid rules and principles can be considered a breach of a cooperation agreement and, consequently, the Company may cancel the contract with the Contracting Partner immediately, while the Contracting Partner shall be obliged to compensate the Company for any damage demonstrably incurred by the Company.

I, the below signed External Employee, hereby acknowledge that:

- (i) My activities connected with the IS are monitored due to the special nature of the business pursued by the Company, and access to separate information systems and to the Internet are logged for security reasons; Email communication sent outside KB and the SG Group, as well as uploading data to web repositories, web emails and social networks, is monitored. The aim of the monitoring is to protect client data and ensure that sensitive information does not leave the bank. This obligation is imposed on the bank by legislation. The monitoring automatically searches for chains that would indicate that the client's sensitive data such as client identification data, credit card numbers, internal data on the client's financial situation evaluation, etc. are leaving the bank. If the search algorithm evaluates a possible violation of the information handling rule, it is forwarded to the SOC for further investigation.
- (ii) The Company owning the information system with which I work or shall work shall process my personal data for the purposes connected with the security of the Company's IS and registering in the HR system for the duration of the contractual cooperation with the Contractor and for the subsequent ten years.

The Company has informed me that:

- (i) The processing of the below personal data is a legitimate interest of the Company and may be objected to; *Note: If the External Employee has entered into the Contract with the Company in person as a Contracting Partner, it is, from the point of view of the registration in the HR system, a statutory performance of the Contract without the right to object;*
- (ii) I shall be entitled to ask the Company for access to my personal data processed by the Company;
- (iii) I shall be entitled to ask that the recorded personal data be corrected or deleted, or their processing be limited;
- (iv) I shall be entitled to approach the Office for Personal Data Protection (if the Company breaches its duties).

This document has been made out in two counterparts, of which the Company shall receive one and the External Employee one.

By my signature hereto, I hereby confirm that I have familiarised myself with the above regulations and duties.

In _____, dated _____

To be filled in by the External Employee

Surname, first name, title:

Personal identification number (Birth number or date of birth):

Telephone number (GSM): _____ (This telephone number shall be listed in the KB list of contacts)

Permanent residence address:

Contracting partner:

Signature of the External Employee

To be filled in by a representative of the Société Générale Group's Company

Société Générale Group's Company:

Company department/division:

Company's Responsible Employee (senior manager with personnel authorities - surname, first name, title):

Workplace address:

Activity performed for the Company:

Starting date of the activities:

Expected date of the completion of the activities:

Duties of external specialists using the Information System

- Tick off if you need to make out a paper ID card of the external specialist.** Please attach a 3.5 x 4.5 cm photograph of the card holder (usual size of an ID or passport photo) to the application. The photograph must reflect the card holder's current appearance.

Signature of the Company's Responsible Employee