SIPRAL a.s. Třebohostická 5a/3165, 100 00–Prague–10 CZ, tel. +420 296 565 111,
sipral@sipral.com

Principles of Personal Data Processing at SIPRAL a.s.

Prepared by	Approved by
Mgr. Lucie Jislová	Leopold Bareš
Company Lawyer	CEO
Directive Validity	Validity of revision
May 25, 2018	28.03.2024

SIPRAL a.s. Třebohostická 5a/3165, 100 00–Prague–10 CZ, tel. +420 296 565 111,
sipral@sipral.com

amendment sheet

Date of amendment	Processed by	Description
25.10.2019	Lucie Jislová	update of chap. 2.3.2. b/ CCTV
14.11.2019	Lucie Jislová	Rules for monitoring premises using CCTV, handling CCTV footage, joint management of personal data.
06.03.2024	Lucie Jislová	Rules of personal data processing in the operation of the security access system for the registration and entry of persons to the premises of the headquarters of SIPRAL a.s. in Třebohostická Street. and production area in Jirny
28.03.22024	Lucie Jislová	Use of cookies on the website

SIPRAL a.s. Třebohostická 5a/3165, 100 00–Prague–10 CZ, tel. +420 296 565 111,
sipral@sipral.com

Table of Contents

SIPRAL a.s. Třebohostická 5a/3165, 100 00–Prague–10 CZ, tel. +420 296 565 111,
sipral@sipral.com

1 General provisions

1.1 Goal and applicability

This document is addressed to all of our business partners and clients (and/or their representatives) and its purpose is to inform you about the basic principles that we at SIPRAL a.s., with its registered seat at the address Třebohostická 3165/5a, Prague 10 – Strašnice, Postal Code: 100 00, ID No.: 61860433, registered in the Commercial Register administered by the Municipal Court in Prague, Section B, File No. 2940 (hereinafter referred to only as "SIPRAL" or "our company") honour and observe in connection with personal data processing (hereinafter referred to as the "Principles").

These Principles reasonably apply also to processing of Personal Data performed by our subsidiary SIPRAL UK Ltd., with its registered seat at the address Bengal Wing, 9A Devonshire Square, London, England, EC2M 4YN, United Kingdom, id. No. 05677591 (hereinafter referred to only as "SIPRAL UK") and our parent company LBSH a.s. with its registered office at the address Třebohostická 3165/5a, Praha 10 – Strašnice, 100 00, IČ: 08044562 (hereinafter as a „LBSH") in the situations when SIPRAL, SIPRAL UK and LBSH carry out joint control over the processing of your Personal Data for certain jointly defined processing purposes and thus are in the positions of so called joint controllers of your personal data (see below in these Principles).

If we speak about "you" and about "our business partners" in these principles, we also mean any and all natural persons representing legal entities in the position of our business partners and clients, i.e., in particular members of statutory bodies, employees of such companies, and other agents.

These Principles have been created on the groundwork and within the scope defined in applicable legal regulations, in particular within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to only as the "GDPR").

In this document, you are going to learn:
- who is the controller of your personal data;
- why do we process your personal data;
- what personal data we process about you;
- how and/or from where do we obtain your personal data;
- how do we process your personal data;
- whom can we provide with your personal data;
- for how long do we process your personal data;
- how is your personal data secured;
- what are your rights with respect to protection of your personal data;
- where can you exercise your rights in relation to the protection of your personal data and where can you obtain up-to-date wording of these Principles of Personal Data Protection;
- what is the situation with electronic communication means and mobile applications;
- what is the validity and effectiveness of these Principles of Personal Data Protection.

Please read the contents of these Principles carefully.

2 Principles

Our company has a number of legal obligations that that relate to processing of personal data of natural persons and that we have to observe mainly with regard to the performance of our contractual obligations, obligations imposed by legal regulations and/or obligations towards public authorities. In this respect, we have to point out that we would be unable to offer or provide our products or services or, on the contrary, purchase/use your or your company's products or services without the provision of certain personal data. Our company processes the personal data of its business partners also due to the performance of executed business agreements and due to legitimate interests of our company or third parties. If we would like to process your personal data for other reasons, we would need your prior consent / consent of the affected natural person with such processing.

We observe mainly the following principles during personal data processing:
a/ we always process the personal data for clearly and comprehensibly defined purpose, using defined means, defined methods, and only for the term necessary with regard to the purpose of its processing;
b/ we process and protect personal data in a way that prevents unauthorized or random access to such personal data, its change, destruction or loss, unauthorized transmission, its alternative unauthorized processing, as well as other misuse;
c/ we inform you comprehensibly about the principles of personal data processing and about the right to accurate and complete information about circumstances of such processing, as well as about other related rights;
d/ we adopt and maintain corresponding technical and organizational measures to ensure security of your personal data; any and all persons that come into contact with your data in connection with its processing are bound by the confidentiality obligation.

2.1 Who is the controller of your personal data?

Controller of your personal data is company SIPRAL a.s., with its registered seat at the address Třebohostická 3165/5a, Prague 10 – Strašnice, Postal Code: 100 00, ID No.: 61860433, registered in the Commercial Register administered by the Municipal Court in Prague, Section B, File No. 2940. Situations, when your personal data is controlled in so called joint control regime, are discussed in Section 2.10. hereof.

2.2 Why do we process your personal data

In this chapter, you will find out what are the purposes for processing your personal data and what is the legal groundwork for such processing. At the same time, we will explain to you what is the difference between processing of your personal data without your consent and the cases when we process your personal data with your consent.

2.2.1 Processing of personal data without consent

We process the personal data without your consent mainly in situations when you are obliged to provide us with certain data as a prerequisite for execution and due performance of relevant

contractual relationship with you or with your company. We are authorized to process your personal data without your consent mainly for the following reasons:

a/ compliance with our legal obligations applicable to us pursuant to relevant legal regulations (acts, decrees, international treaties, or Commission Regulations), including, but not limited to, the following purposes:
- accounting and tax records;
- administration of contractual documentation;
- proving the professional qualification and competence;
- recording and identification of persons entering the construction site, business premises, or production premises of our company;
- recording of protective equipment as a part of compliance with OHS conditions at work;
- assurance and recording of OHS and FP trainings;
- documenting, recording, and investigation of offences or other incidents during work performance;
- registration of occupational injuries;
- registration and issue of product and transport note, delivery note, product shipping confirmation;
- registration of construction logs and other operating logs;
- registration of forklift drivers, truck drivers, or drivers of other transport means requiring a special driver's license;
- recording of persons who perform specialized works (work at heights, etc.);
- prevention of damages to property of our company, our customers, as well as third parties;
- prevention of fraudulent actions;
- fulfilment of other notification duties towards public authorities;
- fulfilment of obligations relating to exercise of judgements, distraints, or insolvency proceedings;
- fulfilment of archiving duties.

b/ legitimate interests of our company, our customers or third parties and/or based on an executed agreement, in particular for the following purposes:
- recording contact details of our business partners' representatives;
- recording and administration of contractual, technical, or other so called job documentation;
- assurance of accommodation or travel documents for our business partners;
- internal comparison of offers from our business partners;
- orders of materials and other commodities;
- provision of information about operation of our company, social events organized by the company, and other major events involving our company;
- products tracing and tracking, order management;
- protection of property of our company, our customers, as well as third parties;
- to ensure the operation of the security access system for the registration and entry of persons into the premises of SIPRAL a.s. in Třebohostická ul. and in the production area Jirny.

2.2.2 Processing of personal data with your consent

We process the personal data with your consent in situations when there is no legitimate reason (as listed above) for the processing of your personal data and when you voluntarily agreed with processing of the personal data that you provided to us.

2.3 What personal data we process about you

In this section, we will explain what personal data we process about you. We will in particular explain the categories into which we divide your personal data – this way, you will better understand not only the scope of your personal data processing but also its purpose.

2.3.1 Basic categories of processed personal data

Our company processes your personal data within the scope necessary for achieving the above-mentioned purposes. We process in particular the identification and contact details, data necessary for deciding about execution of relevant agreement, data produced as a part of performance of contractual obligations under the agreement with our company, data relating to provision of our products and services, data created by our own activities and to necessary and legitimate extent also similar data about other persons whose personal data is important for us in connection with contractual (or other legal) relationship between you and our company. This way, our company processes mainly the following personal data:

a/ identification details – identification details means data which allow us to identify you so we can execute relevant agreement with you and/or your company or provide you with or offer to you our products and services and/or purchase your products and use your services; such details include in particular your name, surname, date and place of birth, in case of clients - natural persons - also ID No. and VAT ID No., birth number, address of permanent residence, type, number, and validity of identity card;

b/ contact details – contact details mean the data that allow us to establish contact with you and communicate with you and/or with your company, i.e., in particular the postal address (if different from the address of permanent residence), telephone number, e-mail address, or other contact details provided by you;

c/ data necessary for decision about contract execution and performance – this comprises such data which allows us to perform our legal obligations defined in connection with execution of relevant agreement. Such data includes in particular information about your professional qualification and work position within your company.

2.3.2 Specific categories of processed personal data

In connection with the personal data that we process, we consider it important to expressly inform you about certain categories of personal data and methods of its processing.

a/ communication records – our company monitors and archives electronic communication by backing-up the contents of e-mail mailboxes of its employees; in this respect, we also back-up the e-mail communication with you as a person and/or with your company. In all these cases, the contents of all communication records is strictly confidential, i.e., our records in no way deal with the contents of such communication and we use the collected data exclusively for the compliance with our legal obligations, for execution and/or performance of agreements, and for our legitimate interests.

b/ CCTV recordings - our company monitors the movement of persons by means of a CCTV system (i.e., by means of video recording) in specific premises of its headquarters and production facility at Jirny; CCTV cameras are located within the premises of our company exclusively for the purpose of protecting the property of SIPRAL a.s. and the lives and health of persons moving within the monitored areas and also for the purpose of controlling the entry/exit of persons to/from the premises of SIPRAL a.s. (to the company's headquarters in Třebohostická street and to the production hall in Jirny); secondarily also for the purpose of monitoring the possible misuse of the emergency leakage and fire alarm for leaving the SIPRAL premises.. Layout of individual CCTV cameras may not interfere with the privacy of the monitored persons, so if you have any doubts about compliance with this rule, please contact the person responsible for personal data protection agenda (see Section 2.11.).

The specific number and layout of individual CCTV cameras within the company premises is shown on the attached layout plan (see Annex to these Principles). When entering the monitored areas, you will be informed about the presence of CCTV cameras by an information sign with a pictogram of CCTV camera.

Our company can use the CCTV camera recordings only in connection with an event resulting in threat or damage to the property of SIPRAL a.s., or any threat to life and health of persons moving within the premises of our company or in connection with checking the identity of persons entering/leaving the premises of SIPRAL a.s.. CCTV camera recordings are archived for 10 days from the date of their creation, because of the need to ensure that records are also kept when company-wide leave is taken, production is shut down or to detect loss and damage to property, except for situations when a recording is requested by any of the public authorities or law enforcement agencies during this period or the record is reviewed in order to investigate or prevent the occurrence of incidents in the operation of SIPRAL a.s. or the record is stored for the purpose of collecting and preserving evidence to resolve an insurance claim; in such case, the recordings shall be archived for any period necessary for the proceedings.

We protect the entire CCTV system (i.e., recording devices, transmission paths and data storage systems) against unauthorized access or other unauthorized processing of personal data, both by encrypting the video recordings and by recording the history of access to the system, and further by securing the physical access to the server room where the data repository is located (i.e. in a lockable room). Only the employees of the company in specific positions have access to the CCTV system recordings – namely Chairman of the Board of Directors, Production Director, Facility and IT Director, Logistics Manager, Production Project Manager, Occupational Health and Safety Technician and QHSE Manager, IT staff and Data Protection Officer. Only the Production Director, Facility and IT Director and the IT staff are authorized to make copies of the recordings in case of registered incidents and submit those to state authorities or law enforcement authorities.

c/ security system for registration and entry of persons into the premises of SIPRAL a.s. - the security access system is installed at all entrance doors to the headquarters of SIPRAL a.s. in Třebohostická street. and in the production hall in Jirny, in order to control and register the entry/exit of persons to/from the buildings of SIPRAL a.s. and to ensure the protection of the property of SIPRAL a.s. The basic tool of the security system is a sensor, which is used to identify a person and then open

the entrance door to the building. The sensors of the access control system do not store fingerprint images, scans or other biometric data in a form that allows for further processing or retrospective reconstruction of such data (i.e. it is not a processing of a special category of personal data within the meaning of Article 9 GDPR), thus the risk of misuse of biometric data is excluded. The security access system is based only on the principle of converting biometric data into numerical expressions, 'numerical templates', which represent a unique numerical identifier. The conversion to numeric templates is always carried out within the technological sensor directly on the sensor and does not allow a backward reconstruction to biometric data. The supplier and guarantor of the technological solution of the security access system is a company EFG CZ spol. s r.o., Zelený pruh 1560/99, 140 00 Prague 4, ID No.: 25649876, registered in the Commercial Register at the Commercial Register of the Ministry of Industry and Trade in Prague, file No. C 58052.

Within the operation of the security access system and from the GDPR point of view, the name, surname and number template assigned to a specific person are processed, in order to enable entry/exit to/from the premises of SIPRAL a.s. on the basis of the identification of the person. Our company is the controller and processor of said personal data. The processing of said personal data will take place for the duration of your contractual relationship with our company, or for as long as you use the security system for entry/exit to/from the premises of SIPRAL a.s. and for this reason you will be assigned a numerical template. The protection of the entire security system (i.e. sensing devices, transmission paths and data storage) against unauthorized access or other unauthorized processing of personal data is ensured by means of authentication of access to the SWF system, as well as by means of physical security of the server room where the data storage is located (i.e. in a locked room). Access to personal data processed in the operation of the security access system is only available to employees of our company in specific positions, namely the Director of Facilities and IT, IT staff, Maintenance Technician and Facility Manager.

The location of the individual sensors is shown on the attached plan (see appendix to this Policy).

d/ use of cookies on our website - we use cookies on our website www.sipral.com. In this context, we have prepared a Special Privacy Policy on the use of cookies (Cookies Policy), which explains what cookies are, why we use them, how you can control the use of cookies by setting your preferences, what types of cookies we use, for what purpose, who is their provider and for how long we keep your personal data. When you first visit our website, you will be asked to consent to the use of cookies, which includes your right to refuse consent or to choose your own settings (preferences) for the use of cookies. You can change your preferences at any time.

2.4 How and from where we obtain your personal data

Our company obtains the personal data mainly:
a/ from its business partners, directly during a tender or when executing an agreement with our company, as well as during the performance of obligations resulting from an agreement;
b/ from its own activities by processing and evaluation of other personal data.

2.5 How we process the personal data

Our company processes your personal data manually. The main purpose of this processing is to comply with our legal obligations and to protect the rights and legitimate interests of our company, our business partners and clients, as well as third parties.

Only when using cookies on our website do we process your personal data automatically if you have given your consent to such processing (see Cookies Policy).

Your personal data is processed mainly by our employees. Where necessary, we use third parties for assurance of our activities (e.g. in connection with the administration of our website or for booking your accommodation and for travel documents issue) so your personal data can also be processed by third parties. In this context, it is useful to mention that such processing always takes place legally in line with the GDPR.

2.6 Whom we can provide with your personal data

Personal data of our business partners is primarily accessible to the employees of our company (and to persons in similar position) in connection with the performance of their work duties during which it is necessary to use the personal data of our business partners. In this context, our employees (and persons in similar position) can, however, access only such data of our business partners that is necessary for the performance of their work tasks and they are also bound by the confidentiality obligation.

Personal data of our business partners can be further transferred to third parties who participate in processing of personal data of the affected natural persons in situations when we used third parties for the assurance of our activities exclusively on the basis of a contract and while ensuring compliance with the legal conditions of the GDPR.

Third parties who can access your personal data include in particular:
a/ persons whom we use for assurance of activities of our company based on an executed agreement, for example auditors or tax advisors, legal service providers;
b/ persons who ensure technical operations, provide certain services, or operate certain technologies required for our services, e.g., forwarders;
c/ other business partners;
d/ persons through whom we ensure our mutual payment transactions;
e/ persons whom we use to exercise claims of our company and/or to defend against claims of other persons;
f/ persons whom we use for assurance of all legal formalities as stipulated by law and/or when such procedure is suitable due to legitimate interests of our company, our customers, or third parties.

2.6.1 Transfer of personal data without consent

Pursuant to applicable legal regulations, our company is authorized or even obliged to transfer your personal data and/or data of affected natural persons without your consent to:
a/ relevant state authorities, courts, bailiffs, law enforcement authorities for the purpose of fulfilment of their obligations and for the purpose of exercise of judgements;

b/ third parties whom we use to ensure the activities of our company in relation to fulfilment of our obligations stipulated by the legal regulations or executed agreements based on executed agreement.

2.6.2 Transfer of personal data with your consent

Our company currently does not transfer your personal data to any other persons in cases when the processing of your personal data requires your consent except for the processing of your personal data when using cookies on our website (see Cookies Policy).

2.6.3 Transfer of personal data abroad

Your personal data is processed within the territory of the Czech Republic or within the framework of so-called joint control within the territory of the Great Britain. Our company does not transfer any personal data into countries outside the European Economic Area.

2.7 For how long we process your personal data

Personal data is processed only for the time necessary with regard to the processing purpose. Our company continuously assesses whether the need for processing of certain personal data necessary for certain purpose still persists. Whenever we determine that relevant personal data is no longer required for any purpose, for which it was processed, we destroy such data. Regardless of the above-mentioned facts, there is a rule that the personal data, which we process for the purpose of execution and performance of a contract, is processed for the entire term of our business and/or contractual relationship between your company and our company and further for the defined archiving period, usually for 10 years.

2.8 How is your personal data secured

All personal data is secured using standard procedures and available technologies. We use such technical, organizational, and safety measures which ensure that there is no unauthorized access to your personal data or unauthorized intervention into such data. Such measures are subsequently regularly revised and improved with regard to state-of-the-art technology. Basic security measures in our company comprise:

a/ network protection by firewalls, antivirus programs, and limitations in form of domain policies;
b/ limited access to internal databases and to network drives;
c/ password protection of personal computer, mobile phone, or any other IT equipment provided to our employees;
d/ locking of offices;
e/ electronic security system in our premises.

At this point, we would like to expressly mention that any level of securing on our side may prove to be insufficient if the protection of your own personal data is not performed responsibly on your part. We therefore ask you and recommend that you ensure the safety of your data by keeping your unique passwords and other credentials to our services secret and observe the basic security principles. Please, always remember that e-mails, instant chat messages, blogs, and other types of communication with other users are not encrypted in our company. We therefore recommend that you avoid using these forms of communication for provision of any confidential Information.

2.9 What are your rights with respect to protection of your personal data

2.9.1 The following particulars apply in relation to your personal data:

If you provide your personal data on your own, we assume that you are providing it voluntarily. At the same time, we have the possibility to obtain your personal data from other sources than from you. And, also, we do not need your consent with processing of your personal data in some cases - we can process it for other legitimate reasons, including, but not limited to, performance of obligations stipulated by legal regulations, due to performance of a contract executed with our company, or due to legitimate interests of our company, our customers, or third parties.

2.9.2 Right to revoke the granted consent with personal data processing

As indicated above, some of your personal data is processed by us only with your consent. If we wish to process your personal data on the groundwork of your consent, you are not obliged to grant such consent. In such case, of course, we are not going to process your personal data that we are not authorized to process for another legal reason. If you give us your consent with processing of your personal data, you can revoke it at any time. If you revoke the granted consent with personal data processing, we will automatically terminate the processing of your personal data that we process on the groundwork of your consent ant that we are not authorized to process for another legal reason.

In this context, we consider it important to remind you that we process your certain personal data on the groundwork of a different legal reason than your consent. Therefore, there might be the situation when you revoke your consent with processing of your personal data that you granted to us for certain purposes but our company will continue processing the same personal data because we will be authorized or even obliged to continue processing the same personal data for other reasons based on a different legal groundwork.

2.9.3 Right of access to personal data

If you ask us for information relating to the processing of your personal data, we will provide you without an undue delay with all information about whether and what personal data we process about you and possibly also for what purpose, to what scope, to whom it is disclosed, from whom we obtained such data and for how long we have been processing it. In this context, we will also inform you about your rights relating to the protection of such personal data of yours and about other facts that we are obliged to communicate to you.

2.9.4 Right to correction or amendment to the personal data

If you find out or believe that your personal data processed by our company is inaccurate or incomplete, you can ask us for its correction or amendment. If we find your request substantiated, our company and/or third party participating in the processing of your personal data will immediately ensure remedy free of charge.

2.9.5 Right to limitation of personal data processing

You have the right to request that we limit the processing of your personal data in any of the following cases:

a/ you believe that your personal data processed by us is inaccurate, for the time that we need to verify the accuracy of relevant personal data;

b/ processing of your personal data is illegal, you refuse deletion of your personal data and request limitation to its use instead;
c/ our company no longer needs such personal data for relevant processing purposes, however, you require it for identification, exercise, or defending your legal claims;
d/ due to the reason relating to your specific situation, you raise an objection against processing of your personal data, processing of which is necessary for fulfilment of a task performed in public interest or for exercise of authority assigned to our company and/or for legitimate interests of our company or a third party, with the exception of cases when your interests or your fundamental rights and freedoms prevail over such interests (including profiling for the above-mentioned purposes) until it is verified whether or not the legitimate reasons of our company prevail over your legitimate reasons;

(any of the above-mentioned cases is hereinafter referred to only as the “disputable question”).

If, in any of the above-mentioned cases, you exercise your right and ask us to limit the processing of your personal data, in such case and for the term specified above (and/or for the term necessary for assessing and resolving relevant disputable issue) we will limit the processing of your personal data and your personal data will be – with the exception of its storage – processed only with your consent with such processing and/or for the purpose of determination, exercise, or defending of legal interests, for protection of rights of another natural person or legal entity, or due to an important public interest. If the reasons for the above-mentioned limitation for processing of your personal data cease to exist, we are authorized to cancel such limitation of personal data processing. This will be communicated to you in advance.

2.9.6 Right to object against the processing of personal data

If we process your personal data on the groundwork of a legitimate interest or in performance of tasks in public interest, you have the right to object against such processing of your personal data.

We will not process your personal data until we assess your objection, with the exception of cases when such processing is necessary for the purpose of determining, exercising, or defending a legal title. In other cases, we will refrain from processing of your personal data until (and unless) we prove the serious legitimate reasons for its processing that would prevail over your interests or over your rights and freedoms.

If we process your personal data for direct marketing purposes, you have the right to object against the processing of your personal data for such marketing purpose (including profiling) as far as direct marketing is concerned. And if you raise such objection in this case, your personal data will no longer be processed for these purposes.

2.9.7 Right to request personal data portability

If we process your personal data by automatic means on the groundwork of your consent or due to performance of a contract executed between you and our company, you have the right to obtain such personal data of yours in a structured, commonly used, and machine legible format. If technically feasible, you also have the right to request that we pass such data to another controller.

2.9.8 Right to be informed about breach of personal data securing

In the event of a breach of your personal data securing with a high risk for your rights and freedoms, you have the right to request that we notify you of such fact without an undue delay.

2.9.9 Right to personal data erasure (right to be forgotten)

If (i) your personal data is no longer required for the purposes for which it was collected or otherwise processed, (ii) processing of your personal data is illegal, (iii) you raise objections against processing of your personal data and there are no prevailing legitimate reasons for its further processing or if you raise an objection against processing of your personal data for direct marketing purposes, (iv) we are required to comply with a legal obligation, or (v) you have revoked your consent based on which your personal data was processed and there is no other legal reason for its processing, you have right to erasure of your personal data and our company is obliged to erase and permanently destroy your personal data. The above-mentioned right does not relate to the processing necessary for (i) exercise of right to freedom of speech and information, (ii) compliance with a legal obligation which requires processing of your personal data or fulfilment of a task in public interest or in the exercise of public authority assigned to our company, (iii) due to a public interest in the area of public health, (iv) for the purpose of archiving in public interest, for the purpose of scientific or historic research, or for statistical purposes if it is likely that your right to erasure would disable or seriously threaten the fulfilment of the goals of such processing, or (v) for determination, exercise, or defending a legal title.

2.9.10 Right to file a complaint against processing of your personal data including method of handling the right to personal data protection exercised by you

If we conclude that your request, by which you exercise your rights, does not meet the requirements necessary for its positive processing, we may reject your request.

In such case, you have the right to file a complaint against processing of your personal data including method of handling the right to personal data protection exercised by you in relation to the protection of your personal data.

You can address such complaint to the supervisory authority:

Úřad pro ochranu osobních údajů (Office for Personal Data Protection)
Pplk. Sochora 27
170 00 Prague 7

More details about the current method of filing your complaint, please refer to the website of the authority at www.uoou.cz

2.10. Joint Control

As we have already mentioned in the introduction into these Principles, SIPRAL, SIPRAL UK and LBSH sometimes perform joint control over processing of your personal data for certain jointly defined processing purposes and thus are in the position of so called joint controllers with respect to your personal data.

This applies to the processing of your personal data for the following processing purposes:

a/ management of IT resources and IT system;
b/ agenda of the Sales Department;
c/ marketing;
d/ OHS agenda for projects executed in the UK;
e/ facility management (relating to the buildings and vehicles);
f/financial controlling;
g/ legal support;
h/ setting up and managing the financing of economic activities.

Due to the joint control over the processing of your personal data for the above-mentioned processing purposes, and due to their positions of joint controllers, SIPRAL, SIPRAL UK and LBSH have entered into an agreement (hereinafter referred to only as the "Agreement on Joint Control of Personal Data"), by which they defined their mutual relationship of the joint controllers and determined the responsibility for the performance of the obligations pursuant to the GDPR in order to ensure that your (data subject's) data processed by the SIPRAL, SIPRAL UK and LBSH as joint controllers remains protected.

SIPRAL took over responsibility for the performance of the following obligations based on the Agreement on Joint Control of Personal Data:

a/ informing data subjects about their rights under the GDPR relating in particular to:

(i) identity and contact details of the controller,
(ii) purpose and legal groundwork of personal data processing,
(iii) categories of processed personal data,
(iv) legitimate interests of the controller if the processing of personal data is necessary for the purpose of legitimate interests of the Contractual Party or third party,
(v) categories of personal data recipients,
(vi) term for which the personal data will be stored,
(vii) existence of the right to request the controller to provide access to personal data, request its correction, deletion, or limitation to processing, right to object against the processing, and right to data portability,
(viii) existence of the right to revoke the consent with personal data processing at any time,
(ix) existence of the right to file a complaint with supervisory authority,
(x) fact whether the personal data provision is based on legal or contractual requirement and whether the data subject is obliged to provide the personal data and possible consequences of rejection to provide such data,
(xi) fact whether automated decision making including profiling takes place;

b/ settlement of rights of the data subject exercised pursuant to the provisions of Articles 15 to 22 of the GDPR;

c/ communication with the supervisory authorities;

d/ execution and performance of agreements on processing of personal data with individual processors;

e/ fulfilment of the notification obligation in case of breach to personal data securing in terms of Articles 33 and 34 of the GDPR to the supervisory authority and to subject of the personal data.

f/ processing of personal data for the following purposes:

(i) IT equipment and IT system administration involving in particular administration of joint network, administration of e-mail mailboxes, security access system and recording of IT resources;

(ii) activities of Sales Department relating in particular to preparation and processing of tender offers;

(iii) marketing agenda relating in particular to marketing communication and public relation (maintenance of the website and administration of social network profiles);

(iv) legal support.

SIPRAL UK took over responsibility for the performance of the following obligations based on the Agreement on Joint Control of Personal Data:

a/ processing of Personal Data for the following purposes:

(i) Sales Department agenda relating in particular to search for new projects in the UK, negotiation, conclusion, and administration of business agreements executed by SIPRAL UK and keeping contact details of business partners' representatives in the UK;

(ii) OHS agenda for projects executed in the UK relating to employees and external contractors in the matters relating to control of access to the construction site and injury records maintenance.

LBSH took over responsibility for the performance of the following obligations based on the Agreement on Joint Control of Personal Data:

a/ processing of Personal Data for the following purposes:
(i) facility management (relating to the buildings and vehicles operated by our company)
(ii) activities of financial controlling and preparation of documents for meetings of the Company's statutory bodies,
(iii) setting up and managing the financing of Company's economic activities.

Contact point for the data subjects in cases of personal data processing which fall under joint control of SIPRAL, SIPRAL UK a LBSH has been determined to be:

Registered office of SIPRAL a.s., address: Třebohostická 3165/5a, Prague 10, Strašnice, Postal Code: 100 00. Person in charge of agenda of joint controllers is currently:
Lucie Jislová, company lawyer, e-mail: lucie.jislova@sipral.com

Regardless of the concluded Agreement on Joint Control of Personal Data and division of responsibilities for the performance of the obligations pursuant to GDPR between SIPRAL, SIPRAL UK a LBSH, you have the right to exercise your rights specified in Section 2.9 hereof at each of the joint controllers and towards each of them.

2.11 Where you can exercise the rights in relation to the protection of your personal data and where you can obtain up-to-date wording of these Principles of Personal Data Protection;
In case of any question relating to the protection of your personal data or if you wish to exercise any of your rights relating to the protection of your personal data, you can do so in person at the registered seat of our company or by written notice sent to the e-mail address of employee in charge of the personal data protection agenda.

Person in charge of the personal data protection is currently:
Lucie Jislová, company lawyer, e-mail: lucie.jislova@sipral.com

Up-to-date wording of these Principles of Personal Data Processing is available at our company website (www.sipral.com) or can be requested from the employee in charge of the personal data protection agenda. In connection with the exercise of your rights relating to the protection of personal data, we can request you (mainly for the purpose of protecting your rights) that you identify yourself in a suitable way so we can verify your identity. This is a security measure which will ensure that your rights relating to the protection of your personal data can only be exercised by the authorized person and that we will prevent any unauthorized persons from accessing your personal data. Such proof of identity can have the form of submitting your identity card, using an officially certified signature, using a recognized electronic signature, or otherwise - depending on the communication method that you choose for communication with us.

2.12 Electronic communication means and mobile application
You can use modern electronic communication means in connection with our business relations and offering of our products and services. This includes in particular utilization of the remote access over the internet and/or utilization of social networks. Due to the special and confidential nature of our products and services, we make sure that your personal data receives adequate protection also during the use of electronic communication means and mobile applications.

2.12.1 Social networks
Our company can communicate with you over various social networks, in particular in connection with our marketing activities involving promotion of our company and/or offering of our products and

services. Prerequisite for such communication is that both our company and you have agreed to the terms and conditions of use of such social network and that we really use such social network. In this context, it is necessary to point out that our communication is addressed to all unidentified persons using the particular social network, including the persons who individually and voluntarily subscribed to the posts of our company on the particular social network and/or individually and voluntarily expressed their will to be informed about the activities of our company on the particular social network. All such communication, provision and reception of which is subject to the terms and conditions of the particular social network, including the terms and conditions relating to the protection of your personal data, is defined by the particular social network.