Approved: 1st September 2020

STICHTING BELARUS SOLIDARITY FOUNDATION

GENERAL PERSONAL DATA PROTECTION POLICY

CONTENT

ANNEXES

I. GENERAL PROVISIONS

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis, including employees, independent contractors, volunteers, applicants, activity partners and other individuals SBSF dealing with.

In this regard SBSF adopts this General Personal Data Protection Policy (hereinafter – "**the Policy**") to regulate the issues related to and arising from collecting and processing of personal data.

The Policy contains:
(1) provisions on basic rules of collecting and processing of personal data,
(2) provisions on collecting and processing of personal data for social marketing purposes,
(3) provisions on collecting and processing of personal data for employment-related purposes and dealing with individual contractors,
(4) provisions on collecting and processing of personal data when dealing with activity partners.

II. SCOPE

The Policy relates to any personal data created, collected or processed by SBSF, whether by electronic or manual means (i.e., in hard copy, paper, or analog form).

The Policy is a foundation of privacy in SBSF and describes the approach taken in any affiliated legal entity of SBSF established and operating anywhere in the world. The Policy should be duly adopted by all employees and individual contractors of such affiliated legal entities according to the procedure provided thereof.

The matters, which arise from privacy matters of applicants related to use of SBSF web-sites and mobile applications for provision of services, charity and other help to the applicants are regulated by the Terms and Conditions of Use of the Web-sites and Mobile Applications of SBSF www.bysol.org/data_protection.

III. TERMS AND DEFINITIONS

SBSF means Stichting Belarus Solidarity Foundation and all legal entities affiliated to Stichting Belarus Solidarity Foundation established and operating anywhere in the world.

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural living person.

Data subject means any identified or identifiable natural person whose personal data is collected and processed by SBSF.

Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

HR personal data means personal data collected and processed by SBSF in an employment context.

Activity Personal Data means personal data collected and processed by SBSF in an activity context or in the course of provision services, charity and other help to the applicants (except of HR personal data).

Terms and Conditions of Use of the Web-sites and Mobile Applications means a set of rules regulation of use of the web-sites and mobile applications published by SBSF (available with following the link www.bysol.org/data_protection).

Employees mean exclusively individuals, who are employed by SBSF on the basis of labor contracts with respective establishment of labor relations and mutual rights and obligations arisen therefrom.

Individual contractors mean a professional (natural person or private entrepreneur), who provide any services to SBSF himself/herself under the respective contracts without establishing of any labor relations. Such individual contractors also includes individuals, who has a volunteer's service contracts with SBSF.

Data protection impact assessment (DPIA) means a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights of data subjects resulting from the collecting and processing of personal data by assessing them and determining the measures to address them.

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by SBSF.

IV. PRINCIPLES OF COLLECTING AND PROCESSING OF PERSONAL DATA

When collecting and processing of personal data SBSF is guided by the principles set forth below. In case this Policy does not contain details on the procedure of collection and processing of personal data SBSF should establish and conduct such process pursuant to such principles.

There are the following principles of data collecting and processing:

Fairness meaning that SBSF shall process personal data lawfully, fairly, and in a transparent manner.

Purpose limitation meaning that SBSF shall only collect personal data for a specific, explicit, and legitimate purpose(s). Any subsequent processing should be compatible with such

purpose(s), unless SBSF has obtained the individual's consent or the processing is otherwise permitted by law.

Proportionality meaning that SBSF shall only process personal data that is adequate, relevant, and not excessive for the purpose(s) for which it is processed.

Data integrity meaning that SBSF shall keep personal data accurate, complete, and up-to-date as is reasonably necessary for the purpose(s) for which it is processed.

Lawfulness meaning that all data processing by SBSF shall be performed on one of the following lawful bases: consent, contract, legal obligation, vital interests, public or legitimate interests.

Data retention meaning that SBSF shall keep personal data in a form that is personally identifiable for no longer than necessary to accomplish the purpose(s), or other permitted purpose(s), for which the personal data was obtained.

Data security meaning that SBSF shall implement appropriate and reasonable technical and organizational measures to safeguard personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use, or access. SBSF shall instruct and contractually require third parties processing personal data on its behalf (if any) to: (a) process it only for purposes consistent with the purpose(s) of SBSF for processing; and (b) implement appropriate technical and organizational measures to safeguard the personal data.

Respect to the rights of data subjects meaning that SBSF shall process personal data in a manner that respects individuals' rights under applicable data protection laws.

Accountability meaning that SBSF shall implement appropriate policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of personal data is in accordance with this Policy and applicable data protection laws.

V. RIGHTS OF DATA SUBJECTS

In accordance with the applicable legal provisions SBSF shall guarantee the following rights to data subjects. When establishing and conducting any procedure on personal data collecting and processing SBSF should follow in full these rights.

Right of access means that any data subject may ask SBSF to access all or part of his/her personal data.

Right of correction means that any data subject may ask SBSF to correct all or part of his/her personal data that might be inaccurate or not up to date.

Right of deletion means that any data subject may ask SBSF to delete all or part of his/her personal data, in particular if the personal data is no longer necessary for performing the purposes for which it have been collected, or if data subject withdraws his/her consent to processing of personal data.

Right of objection means that any data subject may object at any time to processing of his/her personal data for the purposes of the legitimate interests pursued by SBSF. However, in such cases SBSF should draw attention of data subjects to the fact that regardless of his/her request, SBSF may have to continue processing his/her personal if there are legitimate or

compelling reasons justifying its processing, or in order to establish, exercise or defend legal rights of SBSF.

Right to limitation means that any data subject may request his/her personal data to be processed in a limited way (no processing, only storage) in the following cases:

(i) for the period required to check the accuracy of his/her personal data following a challenge to the accuracy of his/her personal data;
(ii) if data subject considers that the processing of his/her personal data is illegal and request limited use of personal data rather than deletion;
(iii) if SBSF no longer needs to process personal data of data subject, but SBSF still needs this personal data to record, exercise or defend data subject's rights;
(iv) if data subject objects to processing of his/her personal data and such data subject wants to limit use thereof while checks are carried out to establish whether the legitimate reasons, which SBSF gives justify continued processing of such personal data.

Right to portability means that any data subject may request his/her personal data to be exported to a third party when previously such data subject has given a consent to collection of his/her personal data or when his/her personal data has been collected while performing a contract.

Right to withdraw consent means that any data subject may at any time withdraw his/her consent on processing of his/her personal data, which was previously duly provided to SBSF.

VI. PERSONNEL RESPONSIBLE FOR PERSONAL DATA PROTECTION

For the purposes of managing of privacy matters a personal data protection officer should be appointed in SBSF as well as a specialist responsible for personal data protection matters should be designated in each legal entity affiliated to SBSF. The respective criteria for nomination of such personnel responsible for personal data protection both for SBSF and each of the legal entities affiliated thereto as well as the tailored job descriptions are provided in the annex to this Policy.

SBSF should communicate the name and contact details of personnel responsible for personal data protection to data subjects to fulfill their right to refer with requests and complaints to such personnel.

VII. REGISTER OF DATA PROCESSING OPERATIONS

For the purposes of documenting all data processing operations and to ensure accountability which involves demonstration of the data protection compliance implemented by SBSF under the Policy, SBSF shall maintain the inventory of all the data processing operations in the specific register.

Such register should be established both in SBSF and separately in each legal entity affiliated hereto. The records inserted to the registers of the affiliated legal entities should be transmitted to the register of SBSF on every 6 (six) months basis.

The registers may be handled both electronically (including using special software) or physically (i.e., in hard copy, paper, or analog form) with execution of all necessary measures to follow the principle of data security described in this Policy.

The registers are managed by the personnel responsible for personal data protection in SBSF and the affiliated legal entities affiliated.

The detailed procedure on management of such registers is set forth in the Regulation on the Register on Collecting and Processing of Personal Data and is reproduced in annex hereto.

VIII. ADOPTION AND IMPLEMENTATION OF THE POLICY

Adoption of the Policy by SBSF and further implementation of the Policy by the affiliated legal entities

The Policy should be initially adopted and implemented by SBSF in the present version. In this regard SBSF should follow the procedure established for adoption of internal corporate documents.

Further during 30 (thirty) working days after due adoption of the Policy by SBSF it should be adopted by the legal entities affiliated to SBSF, taking into consideration specific mandatory provisions of the applicable law of the states, where such legal entities are established and operate. In this regard such legal entities should follow the procedure established for adoption of their internal corporate documents.

Adoption of the Policy by the employees of SBSF

SBSF is committed to ensuring that this Policy is observed by all employees of SBSF.

SBSF employees shall comply with this Policy in addition to provisions on personal data protection set forth in the other duly adopted documents regulating personal data protection matters.

All employees of SBSF should be notified on the provisions of this Policy in either of the following ways:

(i) for current employees: during 20 (twenty) working days after adoption of this Policy by the respective legal entity affiliated to SBSF (depending which legal entity is employed with);
(ii) for newly-employed individuals: during 5 (five) working days commencing the beginning of labor relations between SBSF and such individual.

The respective notification should be conducted in written by the personnel responsible for personal data protection in SBSF and the employees of SBSF should certify their acknowledgement of the Policy with their signatures or in another way that confirms their acknowledgement of the Policy (in hand or in electronic form). The respective records should be inserted to the Register on Collecting and Processing of Personal Data.

Any personal data collected and processed by SBSF or on its behalf falls under the category of confidential information protected in SBSF. Therefore, in case any personal data is illegally disclosed by any employee of SBSF such employee should be brought by SBSF to responsibility in due course and terms according to the internal rules on confidentiality established in SBSF and applicable law.

Individual contractors are not the employees of SBSF and do not fall under the provisions of this Policy, instead all privacy matters related to them are regulated on a contractual basis.

IX. POLICY COMPLIANCE

In order to ensure due implementation and performance of the Policy a set of policy compliance measures is established. Such measures should be managed by the personnel responsible for personal data protection in SBSF.

Compliance measurement

Compliance with this Policy is verified by various means, including the following:

(i) regular internal audits conducted by the personnel responsible for personal data protection in SBSF;
(ii) external audits of the system of personal data protection, which may be requested by activity partners of SBSF or demanded by the state bodies responsible for personal data protection matters and duly authorized thereto;
(iii) self-assessment of following this Policy by the employees of SBSF;
(iv) audits in the process of reviewing requests to SBSF from any data subjects and providing feedback.

SBSF will monitor its compliance with this Policy on an ongoing basis. SBSF will periodically verify that this Policy continues to conform to the applicable personal data protection laws and is being complied with.

Risk Management on Personal Data and Data Protection Impact Assessment (DPIA)

Risk management on personal data includes DPIA procedure and the other procedures taken by SBSF in this regard.

Risk management procedures including DPIA envisage the following procedures:

(i) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by SBSF;
(ii) assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(iii) assessment of the risks to the rights of data subjects;
(iv) measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with personal data protection provisions taking into account the rights and legitimate interests of data subjects.

Risk management procedures including DPIA may concern both a single processing operation of personal data within some legal entity affiliated to SBSF and multiple processing operations which are similar and hold in each legal entity affiliated to SBSF.

Risk management procedures including DPIA should be conducted for each existing and newly-launched activity process in SBSF and all legal entities affiliated hereto.

Risk management procedures including DPIA should be continuously reviewed and regularly re-assessed meaning that SBSF should analyze its activity processes to identify any new elements related to collecting and processing of personal data. All information on conduction of such procedures should be recorded in the Register on Collecting and Processing of Personal Data.

The terms and methodology of carrying out of such risk management procedures including DPIA and the other related procedures are set forth under the Regulation on Risk Management on Personal Data which is provided in the annex to this Policy.

All risk management procedure on personal data including DPIA are initiated and managed by the personnel responsible for personal data protection in SBSF.

X. OPERATIONS RELATED TO DATA COLLECTION AND PROCESSING

Basic rules of collecting and processing of personal data

SBSF should follow the principles of collecting and processing of personal data as well as respect the rights of data subjects in the course of each procedure of collection and processing of the personal data.

SBSF neither collect nor process (1) the special categories of personal data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and (2) personal data of data subject who are below 16 years old. In case such necessity arises it should be notified to the personnel responsible for personal data protection in SBSF. Any collection or processing of such category of personal data is strictly prohibited unless an explicit consent was provided by the authorized personnel, who is responsible for personal data protection in SBSF.

No procedure of personal data processing can be initiated in SBSF without prior defining of the full scope of purposes for this. In SBSF it is prohibited to process personal data for the purposes other than for which such personal data was initially processed unless explicitly agreed by data subjects.

Processing of personal data by SBSF shall be lawful only if and to the extent that at least one of the following applies:

- data subject has given consent to the processing of his /her personal data for one or more specific purposes (where applicable SBSF should use its template of the respective consent set forth in the annex to this Policy);
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (where applicable SBSF should use its template of the respective contractual provision set forth in the annex to this Policy);
- processing is necessary for compliance with a legal obligation to which SBSF is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in SBSF;
- processing is necessary for the purposes of the legitimate interests pursued by SBSF or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

No procedure of personal data processing can be initiated in SBSF without clear understanding of the legal basis of such processing.

The information on establishment of designated purposes and proper legal grounds for each category of both single and multiple processing operations should be recorded in the Register on Collecting and Processing of Personal Data.

The personnel responsible for personal data protection in SBSF should control and manage that all procedures related to personal data collecting and processing in SBSF fall under the designated purposes and were grounded on the respective legal basis.

Collecting and processing of personal data for social marketing purposes

The following categories of social marketing activities require collecting and processing of personal data:

Purposes	Legal basis	Instructions
Personal data received in the course of social marketing activities	Consent Legitimate interest of SBSF	Prior to involvement of data subject to any social marketing activities consent on personal data processing should be received (with template of such consent set forth in the annex to the Policy). Unless consent cannot be received, personal data can be processed on the basis of legitimate interest of SBSF, but it should not prevail under the legitimate interest of data subjects and they can prohibit use of their personal data anytime.
Personal data for sending newsletters and social advertisement on the services of SBSF, charity and other help to the applicants	Consent Legitimate interest of SBSF	Personal data can be processed on the basis of legitimate interest of SBSF, but it should not prevail under the legitimate interest of data subjects, who should have an explicit option to unsubscribe from such social marketing activities.
Personal data for communication on surveys	Consent Legitimate interest of SBSF	Personal data can be processed on the basis of legitimate interest of SBSF, but it should not prevail under the legitimate interest of data subjects, who should have an explicit option to unsubscribe from such activities. Data subject may provide

		his/her personal data under the proposed consent (with template of such consent set forth in the annex to the Policy).
Use of the web-sites and mobile applications published by SBSF (including social advertisements, authorization on web-sites and mobile applications)	Consent Legitimate interest of SBSF	All terms of regulation of processing personal data are provided under the Terms and Conditions of Use of the Web-sites and Mobile Applications.

Collecting and processing of personal data for employment-related purposes

When dealing with employment matters the following HR personal data is collected and processed by SBSF:

Purposes	**Legal basis**	**Instructions**
Personal data of the candidates applied for positions	Consent	Consent for processing of personal data should be received simultaneously with provision of CV by candidates (with template of such consent set forth in the annex to the Policy).
Personal data of the current employees	Consent Performance of a contract Legal obligation to which SBSF is subject	Consent for processing of personal data (or the respective provisions under labour contract) should be received simultaneously with establishment of labor relations (with template of such consent/contractual provision set forth in the annex to the Policy). Such personal data may be also transferred (including cross-border data transfers) within SBSF – the respective option should be provided under consent or labor agreement.
Personal data of the former employees	Legal obligation to which SBSF is subject	Some HR personal data on the former employees should be processed for accounting purposes. It's necessary to control the scope of such personal data to further processing, but no extra documents are need for further processing.

Collecting and processing of personal data when dealing with activity partners and applicants

When dealing with any activity partners (including individual contractors) and applicants the following activity personal data is collected and processed by SBSF:

Purposes	Legal basis	Instructions
Personal data of activity partners (including individual contractors)	Performance of a contract Legal obligation to which SBSF is subject	The respective provisions should be included to the contract (with template of such contractual provision set forth in the annex to the Policy).
Personal data of applicants (exclusively for activity matters)	Performance of a contract Consent Legal obligation to which SBSF is subject	The respective provisions should be included to the contract (with template of such consent set forth in the annex to the Policy). Alternatively the consent can be provided to SBSF.

XI. PROTECTION OF PERSONAL DATA IN CASE OF CROSS-BORDER DATA TRANSFERS

The Policy is intended to provide adequate safeguards for the processing of personal data entrusted to SBSF and transferred from countries requiring such protections. This is to enable SBSF to transfer personal data wherever it is needed around the globe to enable and support its internal activity processes or enable provision of its services.

To ensure legitimacy of cross-border transfer of personal data SBSF is obliged to take the following actions:

- if personal data transfers take place to a country outside the European Union, SBSF will put in place measures to protect such personal data, appropriate to the legislation in force (e.g. to receive the respective consent from data subject),
- if personal data transfers take place to the EU where it will be processed in accordance with the legal provisions of the General Data Protection Regulation, SBSF will put in place measures to protect such personal data, appropriate to such legislation.

SBSF is entitled to conduct cross-border transfers of personal data exclusively for the same purposes as it is processed by itself.

SBSF should conduct cross-border transfers of personal data only pursuant to appropriate legal ground, in particular under the respective consent contacting an explicit option of such data transfer.

SBSF is obliged to conclude data transfer agreements each time of conducting cross-border transfers of personal data.

All matters related to cross-border transfers of personal data should be managed by the personnel responsible for personal data protection in SBSF.

All information on cross-border transfers of personal data should be recorded in the Register on Collecting and Processing of Personal Data.

XII. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

SBSF shall disclose personal data of data subjects exclusively to the following categories of third parties:

- partner companies of SBSF (only if data subject previously have agreed to this);
- suppliers of SBSF (to fulfil a task on behalf of SBSF, including sales support, market research or applicant services, and account management, supply of products or services now or in the future, or prize draws, competitions or promotions etc.);
- external providers of personal data processing services;
- to the buyer of SBSF in the event of a takeover;
- to third party when stipulated or authorized by the law, or a valid legislative provision, court order or regulation, or if such disclosure is necessary as part of an investigation or procedure, within the national territory or in another country.

Prior to disclosure of personal data to third parties SBSF should check and control legitimate grounds for personal data disclosure as well as to ensure due legal, organizational and technical measures taken by such third parties for data security. In this regard data transfers agreements should be concluded between SBSF and third parties (where applicable SBSF should use its template of the respective contractual provision set forth in the annex to this Policy).

All matters related to disclosure of personal data to third parties should be managed by the personnel responsible for personal data protection in SBSF.

All information on disclosure of personal data to third parties should be recorded in the Register on Collecting and Processing of Personal Data.

XIII. RESPONSES TO REQUESTS OF DATA SUBJECTS

Upon the respective request made by data subject SBSF is obliged to provide the information on collecting and processing of his/her personal data following such terms:

(i) response should be provided on a free of charge basis (unless requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, thus SBSF may either (1) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, (2) refuse to act on the request) and

(ii) response should be provided without undue delay (meaning at the latest within one month, but that period may be extended by two further months where necessary, taking into account the complexity and number of the requests).

The data subject has the right to obtain from SBSF confirmation as to whether or not his/her personal data are processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing,
- the categories of personal data concerned,

- third parties or categories of third parties to whom personal data have been or will be disclosed, (in particular third parties abroad and the appropriate safeguards in this regard),
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from SBSF rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing,
- the right to lodge a complaint with a supervisory authority,
- where the personal data are not collected from the data subject, any available information as to their source,
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If the request relates to any matter out of the abovementioned scope SBSF is entitled to response that it cannot comply with such request. In such a case SBSF should also provide data subjects with the respective reasons.

Information on any requests of data subjects should be recorded to the Register on Collecting and Processing of Personal Data during 3 (three) working days after receiving of such request.

Any responses to requests of data subjects should be provided exclusively with the template of response set forth in the annex to the Policy and by the personal responsible for personal data protection in SBSF.

XIV. PERSONAL DATA RETENTION

Unless otherwise provided under the Policy or applicable law personal data may only be retained by SBSF as long as necessary for the purpose of processing.

SBSF is obliged to delete personal data in the following cases:

- data subject has withdrawn consent to processing of personal data (unless another valid legal basis has been established and communicated to the data subjects);
- contract has been performed or cannot be performed anymore and there is no need in further retention of personal data;
- personal data is no longer up to date.

SBSF shall follow the obligation mentioned above unless any obligation imposed to SBSF by law appears in this regard.

SBSF accepts such retention times for the following processing activities:

- financial and tax data for the purpose of compliance with tax regulations for the period specified by tax laws;
- newsletter subscribers' information, only until consent is withdrawn by using an "unsubscribe" functionality;
- employee files and records for as long as required by relevant employment and social security and social protection laws;
- applicant’ contract, service, help, charity of SBSF are provided.

When considering the matter of expiration of the applicable retention period SBSF should take note on the information in the Register on Collecting and Processing of Personal Data.

After the expiration of the applicable retention period SBSF should erase the respective personal data within 10 (ten) working days after such expiration. Alternatively SBSF may also take a decision on anonymization of such personal data achieved by the following means:

- erasure of the unique identifiers which allow the allocation of a data set to a unique person;
- erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
- separation of personal data from non-identifying information;
- aggregation of personal data in a way that no allocation to any individual is possible.

Information on any personal data erasure on the basis of expiration of the applicable retention period or anonymization of such personal data should be recorded to the Register on Collecting and Processing of Personal Data during 3 (three) working days after such erasure or anonymization.

The personnel responsible for personal data protection should control and manage the procedures related to personal data retention, further respective erasure or anonymization of such data in SBSF.

In addition the data subject shall have the right to obtain from SBSF the erasure of his/her personal data without undue delay or restriction of processing of personal data. The personnel responsible for personal data protection should determine whether such request can be fulfilled on a case-by-case basis.

XV. COMPLIANCE EXCEPTIONS AND NON-COMPLIANCE WITH THE POLICY. DATA BREACHES

Compliance exceptions

SBSF, all affiliated legal entities, as well as all employees of SBSF shall comply with this Policy.
Any exceptions to this Policy require the written approval of the personnel responsible for personal data protection at SBSF with the respective record of such an approval in the Register on Collecting and Processing of Personal Data.

Non-compliance with the Policy

Deviations or non-compliance with this Policy, including attempts to circumvent the stated policy/process by bypassing or knowingly manipulating the process, system, or data may result in disciplinary actions, including termination, as allowed by internal rules of SBSF and local laws.
Information on any accidents on deviations or non-compliance with this Policy requires a respective record to the Register on Collecting and Processing of Personal Data.

Data breaches

SBSF considers as data breach any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by SBSF.

As soon as SBSF becomes aware that personal data breach has occurred, it should notify respectively the supervisory authority without undue delay, but not later than 72 hours after having become aware of it, unless SBSF is able to demonstrate that the personal data breach is

unlikely to result in a risk to the rights of data subjects. Where such notification cannot be achieved by SBSF within 72 hours, the reasons for the delay should accompany the notification conducted by SBSF further made without undue delay. Such notification should be conducted with use of the notification template provided in the annex to this Policy.

As soon as SBSF becomes aware that personal data breach has occurred, it should also communicate to the data subject without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of data subject. Such notification should be conducted with use of the notification template provided in the annex to this Policy.

The obligations on notification of supervisory authority and data subject are feasible only in case such data breach occurred in those affiliated legal entity of SBSF, which is established and operate in the state with such obligations envisaged under applicable law.

Information on any data breaches or any related risks should be recorded to the Register on Collecting and Processing of Personal Data during 3 (three) working days after such accident took place. Such information should contain at least (1) the facts relating to the personal data breach, (2) its effects and (3) the remedial action taken.

The personal responsible for personal data protection in SBSF should during 3 (three) working days commencing data breach initiate taking of all legal, organizational and technical measures to ensure further data security.

XVI. COMPLIANCE WITH APPLICABLE LAW

SBSF shall comply with applicable local personal data protection laws and requirements in those states where the legal entities affiliated to SBSF are established and operate.

Where applicable personal data protection laws require a higher standard of protection for personal data than set out in the Policy, the requirements of applicable data protection law shall prevail. Where applicable data protection laws establish a lower the Policy, the requirements of this Policy shall prevail.

Where any data subjects have reason to believe that applicable law prevents SBSF from fulfilling its obligations under this Policy, they shall promptly inform the personnel responsible for personal data protection in SBSF via sending a request to the following e-mail address: privacy@bysol.org.

Where there is a conflict between applicable law and this Policy, the personnel responsible for data protection in SBSF shall make a responsible decision regarding what action to take to resolve such a conflict and shall consult with the relevant regulatory authority in cases of doubt.

XVII. UPDATE OF THE POLICY AND ITS EFFECTIVE DATE

The Policy may be reviewed and updated. In such a case SBSF shall:

- take reasonable steps to inform all legal entities affiliated to SBSF, SBSF employees, activity partners, and other data subjects affected by the amendments;
- take necessary actions to implement amendments within the legal entities affiliated to SBSF;

- provide appropriate written notices referring to the amendments and hold written acceptance procedure with SBSF employees to certify their acknowledgement of the amended policy.

The information on any amendments of the Policy shall be recorded in the Register on Collecting and Processing of Personal Data. The Policy is effective upon approval by SBSF.

Annex № 1

PERSONNEL RESPONSIBLE FOR PERSONAL DATA PROTECTION

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis. In this regard SBSF adopted the General Personal Data Protection Policy (hereinafter – "the Policy") to regulate the issues related to and arising from collecting and processing of personal data.

Part VI of the Policy envisages that for the purposes of managing of privacy matters a personal data protection officer should be appointed in SBSF as well as a specialist responsible for personal data protection matters should be designated in each legal entity affiliated to SBSF under the data protection officer (hereinafter jointly - "the Personnel").

This Annex to the Policy regulates the details related to the Personnel.

OBLIGATIONS OF SBSF REGARDING THE PERSONNEL

- given to the Personnel the size and structure of SBSF for proper managing of personal data issues;
- active support of the function of the Personnel by senior management;
- adequate support of the Personnel in terms of financial resources, infrastructure and staff (where appropriate);
- necessary access to other services, such as Human Resources, legal, IT, security departments;
- sufficient time for the Personnel to fulfill their duties;
- official communication of the designation of the Personnel to all staff to ensure that their existence and function are known within SBSF;
- continuous training of the Personnel on data protection issues.

CRITERIA FOR NOMINATION OF THE PERSONNEL

The Personnel shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks.
There are the following requirements:

- knowledge of data protection law and practices (national and European data protection laws and practices including an in-depth understanding of the GDPR);
- understanding of the specifics of activity of SBSF and processing operations of personal data protection carried out within SBSF;
- understanding of information technologies and data security issues;
- knowledge of the system of corporate compliance of SBSF;
- ability to promote a data protection culture within SBSF;
- good command of English.

JOB DESCRIPTION FOR PERSONNEL

General requirements

- to be in position to perform their duties and tasks in an independent manner;
- to be involved properly and in a timely manner in all issues which relate to the protection of personal data in SBSF;

- to act as intermediary between the stakeholders involved to personal data processing procedures;
- to participate regularly in meetings of senior and middle management of SBSF;
- to report to the highest management level of SBSF (i.e. to inform on taken decisions and make annual reports);
- to provide immediate consultation and lead necessary actions once a data breach or another incident has occurred.

Tasks

- to monitor and assess the effectiveness of data protection systems (with conducting: regular internal audit one time per year; interim periodic audits one time per every three months if necessary);
- to monitor compliance with data protection rules and regulations (meaning collection of information, identification of processing activities, analyzing and checking the compliance of processing activities and due regard to the risks associated with personal data processing operation, taking into account the nature, scope, context and purposes of processing);
- to maintain a record of all categories of processing activities regarding personal data carried out on behalf of SBSF and affiliated legal entities with inserting information to the Register on Collecting and Processing of Personal Data;
- to draft, maintain and implement data protection policies and procedures;
- to inform, advise and issue recommendations to SBSF and the affiliated legal entities;
- to notify the employees of SBSF on the provisions of this Policy and the other documents related to data protection issues;
- to carry out all necessary procedures on risk management in respect of personal data and data protection impact assessment (DPIA) procedures (in particular to advise SBSF on whether or not to carry out such procedures, what methodology to follow when carrying out such procedures, whether to carry out such procedures in-house or whether to outsource it, what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of the data subjects in respect of such procedures; whether or not such procedures has been correctly carried out and whether its conclusions);
- to assess risks and take decisions on processing of the special categories of personal data and the personal data of data subject who are below 16 years old;
- to manage cross-border transfers of personal data conducted by SBSF;
- to manage disclosure of personal data to third parties;
- to cooperate with the supervisory authority and act as contact point on data protection matters;
- to respond to data protection requests and complaints received from data subjects and third parties;
- to manage the processes provided under retention policy including the procedures of rectification, erasure of personal data or restriction of processing of personal data;
- to lead necessary actions once a data breach or another incident has occurred;
- to organize and hold trainings for management and staff of SBSF.

PUBLICATION AND COMMUNICATION OF THE CONTACT DETAILS OF THE PERSONNEL

To guarantee easy and direct contact of data subject, supervisory authorities and any third parties to the personnel responsible for personal data protection SBSF and the affiliated legal entities should:

- publish the contact details of the personnel responsible for personal data protection (the dedicated e-mail address shall be published in the Terms and Conditions of Use of the Web-sites and Mobile Applications of SBSF (link);
- inform employees of the name and contact details of the personnel responsible for personal data protection (by sending relevant messages to the emails of such employees or posting relevant messages on the site of SBSF) as well as on the tasks provided by such personnel;
- communicate the contact details of the personnel responsible for personal data protection to the relevant supervisory authorities (if provided by applicable law the name of the personnel responsible for personal data protection and their contact details should be provided).

CONFIDENTIALITY AND PERFORMING TASKS IN INDEPENDENT MANNER BY THE PERSONNEL

SBSF ensures confidentiality for each communication of the Personnel by data subjects or third parties.

The Personnel are bound by secrecy or confidentiality concerning the performance of the respective tasks.

There are the following safeguards to enable the Personnel to act in an independent manner:
- no instructions by SBSF regarding the exercise of the tasks;
- no dismissal or penalty by SBSF for the performance of the tasks of SBSF;
- no conflict of interest with possible other tasks and duties;
- no conflict of interest (the Personnel cannot hold a position within SBSF that leads to determine the purposes and the means of the processing of personal data. Such conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of social marketing department, head of Human Resources or head of IT departments), but also other roles lower down in the organizational structure if such positions or roles lead to the determination of purposes and means of processing);
- no personal responsibility of the Personnel for non-compliance with data protection requirements.

SBSF may disagree with advice of the Personnel. In such a case SBSF should specifically justify in writing why the advice has not been taken into account and the respective record should be included to the Register on Collecting and Processing of Personal Data.

MISCELLANEOUS

SBSF may amend the respective details related to the Personnel for each affiliated entity thereto. In such a case these amended criteria for nomination and job description should be duly implemented in such legal entity according to the procedure provided in Part VIII of the Policy.

Annex № 2

REGULATION ON THE REGISTER
ON COLLECTING AND PROCESSING OF PERSONAL DATA

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis. In this regard SBSF adopted the General Personal Data Protection Policy (hereinafter – "the Policy") to regulate the issues related to and arising from collecting and processing of personal data.

Part VII of the Policy envisages that for the purposes of documenting all data processing operations and to ensure accountability which involves demonstration of the data protection compliance implemented by SBSF under the Policy SBSF shall document all the data processing operations in the specific register (hereinafter – "the Register").

This Annex to the Policy regulates the details related to the Register, which SBSF keeps as data controller.

PURPOSES OF DOCUMENTAION OF DATA RELATED PROCEDURES

- drafting privacy notice – much of the information SBSF has to document is very similar to what you need to tell people in your privacy notice;
- responding to access requests – knowing what personal data is held and where it is will help SBSF to efficiently handle requests from individuals for access to their information;
- taking stock of your processing activities – this will make it much easier for SBSF to address other matters under the GDPR such as ensuring that the personal data SBSF holds is relevant, up to date and secure;
- improve data governance – highlighting and addressing data protection matters through documentation will support good practice in data governance. This can give SBSF assurance as to data quality, completeness and provenance;
- increase activity efficiency – knowing what personal data SBSF holds, why SBSF holds it and for how long, will help SBSF to develop more effective and streamlined activity processes.

ESTABLISHMENT, KEEPING AND UPDATING OF THE REGISTER

The Register should be established both in SBSF and separately in each legal entity affiliated hereto.

The registers are managed by the personnel responsible for personal data protection in SBSF and the affiliated legal entities affiliated.

Before establishment of the Register SBSF should pass data-mapping exercises to feed into the documentation of your processing activities. For these purposes it's necessary to:

- do information audits to find out what personal data SBSF holds;
- distribute questionnaires and talk to staff across SBSF to get a more complete picture of our processing activities; and
- review SBSF policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

Updating of the Register

SBSF conducts regular reviews of the processed personal data and update the documentation accordingly:

- current reviews are conducted in the course of daily operational activities as a case may be;
- full reviews and data audits are conducted once in each 6 months including the stages of (1) data mapping, (2) documenting the results of data mapping to the register, (3) working out decisions for further actions.

The reviews should be initiated by the personnel responsible for personal data protection in SBSF and the affiliated legal entities respectively.

The records inserted to the registers of the affiliated legal entities should be transmitted to the Register of SBSF once in each six months.

FORM AND STRUCTURE OF THE REGISTER

SBSF documents processing activities in a granular way with meaningful links between the different pieces of information.

Form of the Register

SBSF keeps the Register in written and documents processing activities in electronic form to add, remove and amend information easily.

As part of record of processing activities SBSF documents, or links to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.

Structure of the Register

Contact details of the data controller and the related parties:

Controller					
Name and contact details		**Data Protection Officer (if applicable)**		**Representative (if applicable)**	
Name		**Name**		**Name**	
Address		**Address**		**Address**	
Email		**Email**		**Email**	
Telephone		**Telephone**		**Telephone**	

Required areas of documentation:

- activity function;
- purpose of processing;
- name and contact details of joint controller (if applicable);
- categories of individuals;
- categories of personal data;
- categories of recipients;
- link to contract with processor;

- names of third countries or international organizations that personal data are transferred to (if applicable);
- safeguards for exceptional transfers of personal data to third countries or international organizations (if applicable);
- retention schedule (if possible);
- general description of technical and organizational security measures (if possible).

Optional areas of documentation

Privacy Notices
- article 6 lawful basis for processing personal data;
- article 9 condition for processing special category data;
- legitimate interests for the processing (if applicable);
- link to record of legitimate interests assessment (if applicable);
- rights available to individuals;
- existence of automated decision-making, including profiling (if applicable);
- the source of the personal data (if applicable).

Consent
- link to record of consent;

Access Requests
- location of personal data;

Data Protection Impact Assessments
- whether data protection impact assessment required;
- data protection impact assessment progress;
- link to data protection impact assessment;

Personal Data Breaches
- whether personal data breach occurred;
- link to record of personal data breach.

DISCLOSURE OF THE INFORMATION FROM THE REGISTER

The information from the Register can be disclosed in the following cases:
- under request of any departments of SBSF (with due reasoning for such request);
- under request of data subjects (to the extent such disclosure is possible under such request);
- under request of the data protection authorities (if conducted according to the envisaged procedure).

Annex № 3

REGULATION ON RISK MANAGEMENT ON PERSONAL DATA (DATA PROTECTION IMPACT ASSESMENT)

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis. In this regard SBSF adopted the General Personal Data Protection Policy (hereinafter – "the Policy") to regulate the issues related to and arising from collecting and processing of personal data.

Part IX of the Policy envisages an establishment of a system of risk management on personal data, as element of personal data protection compliance in SBSF.

This Annex to the Policy regulates the details of risk management system on personal data taken by SBSF, which includes details on Data Protection Impact Assessment (hereinafter - "DPIA") procedure, its terms and methodology.

STAGES OF RISK MANAGEMENT PROCEDURES

Risk management procedures including DPIA envisage the following procedures:

- systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by SBSF;
- assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- assessment of the risks to the rights of data subjects;
- measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with personal data protection provisions taking into account the rights and legitimate interests of data subjects.

BASIC RULES FOR RISK MANAGEMENT PROCEDURES RELATED TO PERSONAL DATA PROCESSING

- risk management procedures including DPIA may concern both a single processing operation of personal data within some legal entity affiliated to SBSF and multiple processing operations which are similar and hold in each legal entity affiliated to SBSF;
- risk management procedures including DPIA should be conducted for each existing and newly-launched activity process in SBSF and all legal entities affiliated hereto;
- risk management procedures including DPIA should be continuously reviewed and regularly re-assessed meaning that SBSF should analyze its activity processes to identify any new elements related to collecting and processing of personal data;
- all information on conduction of risk management procedures should be recorded in the Register on Collecting and Processing of Personal Data.

PURPOSES AND TASKS OF DPIA

DPIA purposes

DPIA is a process to help SBSF identify and minimize the data protection risks of any project. This is a key part of the new focus on accountability and data protection by design.
To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

DPIA tasks

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

ROLE OF THE PERSONNEL RESPONSIBLE FOR DATA PROTECTION IN DPIA

Scope of responsibilities of the personnel responsible for data protection

The personnel responsible for personal data protection in SBSF are responsible for:

- advising on the following issues:
  - whether you need to do a DPIA;
  - how you should do a DPIA;
  - whether to outsource the DPIA or do it in-house;
  - what measures and safeguards you can take to mitigate risks;
  - whether you've done the DPIA correctly; and
  - the outcome of the DPIA and whether the processing can go ahead;
- documenting the details related to conducting of DPIA:
  - details on conducting DPIA and the respective advice;
  - justification on omitting DPIA procedure under the advice of the personnel responsible for personal data protection in SBSF/management of SBSF/other employees of SBSF/any third parties (with specifying such party);
  - reasoning of SBSF management/other employees of SBSF on omitting the advice of personnel responsible for personal data protection in SBSF, which was provided as DPIA result.
- monitoring DPIA's ongoing performance, including how well SBSF have implemented the planned actions to address the risks.

Third parties involved to DPIA

DPIA procedures can be outsourced under the decision of the personnel responsible for personal data protection in SBSF to:

- the private consultants specializing in data protection sphere;
- data processor conducting processing operations related to the personal data for SBSF.

In such a situation SBSF personnel are still responsible for the results of the DPIA.

Requests to data protection supervisory authorities on DPIA

The personnel responsible for personal data protection in SBSF may also request consultations of the representatives of the respective data protection supervisory authority. In case it was identified that there is a high risk that SBSF cannot mitigate the personnel responsible for personal data protection in SBSF are obliged to request advice both of the private consultants specializing in data protection sphere and the representatives of data protection supervisory authorities prior to starting the processing.

The request to the respective data protection supervisory authority should contain the following:

- a description of the respective roles and responsibilities of any joint controllers or processors;

- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- contact details of your DPO (if you have one); and
- a copy of the DPIA.

SBSF cannot start any data processing operation prior to receiving the response on the request from the respective data protection supervisory authority.

DPIA PROCESS

SBSF initiates DPIA early in the life of a project before the start of processing and runs it alongside the planning and development process.

DPIA steps

1. Identify need for DPIA;
2. Describe the processing;
3. Consider consultations;
4. Assess necessity and proportionality;
5. Identify and access risks;
6. Identify measures to mitigate risks;
7. Sign off and record outcomes;
8. Integrate outcomes into plan;
9. Keep under review.

Details on the basic steps

Step 1 **To identify the need for a DPIA**	The key principle: SBSF must do a DPIA before it begin any type of processing that is "likely to result in a high risk" meaning that although the actual level of risk has not been actually assessed yet, it's necessary to screen for factors that point to the potential for a widespread or serious impact on individuals. SBSF must do a DPIA: 1. for processing that is likely to result in a high risk to data subject There are the following processes which always require DPIA: • systematic and extensive profiling with significant effects; • large scale use of sensitive data; • public monitoring. There are the following criteria either of which acts as indicators of likely high risk processing and identify the operations which fall under DPIA procedure: • evaluation or scoring; • automated decision-making with legal or similar significant effect; • systematic monitoring; • sensitive data or data of a highly personal nature; • data processed on a large scale; • matching or combining datasets; • data concerning vulnerable data subjects; • innovative use or applying new technological or organizational solutions;

<table>
<tr><td></td><td>
preventing data subjects from exercising a right or using a service or contract.
2. for any other major project which requires the processing of personal data.

If there is a change to the nature, scope, context or purpose of personal data processing some new DPIA should be conducted.

If it was decided not to carry out DPIA in any case the respective decision should be documented in the Register on Collecting and Processing of Personal Data with indicating the reasons for such decision.
</td></tr>
<tr><td>Step 2
To describe the processing</td><td>
To describe the processing it is necessary to define (1) how, (2) why it's decided to process personal data with noting:
<table>
<tr><td>Nature
(what is planned to do with the personal data)</td><td>• how collect the data;
• how store the data;
• how use the data;
• who has access to the data;
• who you share the data with;
• whether use any processors;
• retention periods;
• security measures;
• whether are using any new technologies;
• whether are using any novel types of processing;
• which screening criteria you flagged as likely high risk.</td></tr>
<tr><td>Scope
(what the processing covers)</td><td>• the nature of the personal data;
• the volume and variety of the persona data;
• the sensitivity of the personal data;
• the extent and frequency of the processing;
• the duration of the processing;
• the number of data subjects involved;
• the geographical area covered.</td></tr>
<tr><td>Context
(internal and external factors which might affect expectations or impact)</td><td>• the source of the data;
• the nature of your relationship with the individuals;
• how far individuals have control over their data;
• how far individuals are likely to expect the processing;
• whether these individuals include children or other vulnerable people;
• any previous experience of this type of processing;
• any relevant advances in technology or security;
• any current issues of public concern;</td></tr>
</table>
</td></tr>
</table>

		• in due course, whether comply with any GDPR codes of conduct or GDPR certification schemes; • whether have considered and complied with relevant codes of practice.
	Purposes of personal data processing (reason why you want to process the personal data)	• legitimate interests, where relevant; • the intended outcome for individuals; and • the expected benefits for SBSF or for society as a whole.
Step 3 **To consider consultation**	There are 2 options for SBSF in this regard: • to seek and document the views of individuals (or their representatives) unless there is a good reason not to; • not to consult individuals (SBSF should record this decision as part of DPIA, with a clear explanation). Particular cases of considering consultations: • **existing contracts** If the DPIA covers the processing of personal data of existing contacts (for example, existing applicants or employees) SBSF should design a consultation process to seek the views of those particular individuals, or their representatives; • **collection of personal data of individuals, which have not been identified yet** If the DPIA covers a plan to collect the personal data of individuals SBSF have not yet identified, it may be necessary to carry out a more general public- consultation process, or targeted research. This could take the form of market research with a certain demographic or contacting relevant campaign; • **cooperation with data processors** In case SBSF is going to involve data processor, it can be requested for information and assistance. • **cooperation with independent consultants** Any individual consultants may be involved to consideration of consultations (legal experts, IT professionals, sociologists, scientists etc.). If finally, the DPIA decision of SBSF differs from the views of the parties involved to consideration of consultations the personnel responsible for personal data protection in SBSF should document the respective reasons for disregarding the views of such individuals to the Register on Collecting and Processing of Personal Data.	
Step 4 **To assess necessity and proportionality of personal**	The key matter is how SBSF will ensure data protection compliance: • SBSF lawful basis for the processing; • how SBSF will prevent function creep; • how SBSF intend to ensure data quality; • how SBSF u intend to ensure data minimization;	

data processing procedure	• how SBSF intend to provide privacy information to individuals; • how y SBSF implement and support individuals' rights; • measures to ensure your processors comply; • safeguards for international transfers of personal data.
Step 5 **To identify and assess risks**	The following risks for data subjects should be considered when identifying and accessing the possible risks related to processing of personal data: • inability to exercise rights (including but not limited to privacy rights); • inability to access services or opportunities; • loss of control over the use of personal data; • discrimination; • identity theft or fraud; • financial loss; • reputational damage; • physical harm; • loss of confidentiality; • re-identification of pseudonymized data; or • any other significant economic or social disadvantage. In additional security risk should be also assessed: • type of the risk; • sources of the risk; • potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). To assess whether the risk is a high-risk SBSF need to consider both (1) likelihood and (2) severity of the possible harm.
Step 6 **To identify measures to mitigate the risks**	Having identified the risk and their sources the options on their mitigation should be developed. SBSF should be initially guided with the following options for mitigation of the risks: • deciding not to collect certain types of data; • reducing the scope of the processing; • reducing retention periods; • taking additional technological security measures; • training staff to ensure risks are anticipated and managed; • anonymising or pseudonymizing data where possible; • writing internal guidance or processes to avoid risks; • using a different technology; • putting clear data-sharing agreements into place; • making changes to privacy notices; • offering individuals the chance to opt out where appropriate; • implementing new systems to help individuals to exercise their rights. Depending on the case and the specifics of the risks SBSF may develop and implement the other options for mitigation of the risks related to collection and processing of personal data. The respective information should be documented by the personnel responsible for personal data protection in SBSF in the Register on Collecting and Processing of Personal

	Data (noting on the benefits of such options – cost/effectiveness/time etc.).
Step 7 **To sign off and record outcomes**	DPIA outcome report should include: • what additional measures is planned to take; • whether each risk has been eliminated, reduced, or accepted; • the overall level of 'residual risk' after taking additional measures; and • whether any additional consultations are need; • precise final decision on whether the reviewed processing procedure is compliant and whether it is possible to proceed with processing. The personnel responsible for personal data protection in SBSF should document all respective decisions on the outcome stage of DPIA. When finalizing and closing DPIA procedure on any personal data processing procedure the personnel responsible for personal data protection in SBSF should check the following: • the key risks related to the intended processing of personal data have been considered; • the broader data protection obligations have been met. To ensure the principles mentioned above the following check-list should be filled in: • it was confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case; • it was explained why we needed a DPIA, detailing the types of intended processing that made it a requirement; • the document was structured clearly, systematically and logically; • DPIA is written in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms which were used; • the relationships between controllers, processors, data subjects and systems are set out clearly, using both text and data-flow diagrams where appropriate; • it was ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented; • it was explicitly stated how the SBSF is complying with each of the Data Protection Principles under GDPR and clearly explained the lawful basis for processing (and special category conditions if relevant); • it was explained how it is planned to support the relevant information rights of data subjects; • all relevant risks to individuals' rights and freedoms was identified, assessed their likelihood and severity, and detailed all relevant mitigations; • it was explained sufficiently how any proposed mitigation reduces the identified risk in question; • the consideration of any less risky alternatives to achieving the same purposes of the processing, and why they were not chosen

	were evidenced; • the details of stakeholder consultation (e.g. data subjects, representative bodies) were given and summaries of their findings were included; • any relevant additional documents which reference in DPIA, e.g. Privacy Notices, consent documents were attached; • the advice and recommendations of the third parties specializing in data protection were incluwed and it was ensured that the DPIA was signed off by the appropriate people; • a schedule for reviewing the DPIA regularly or when the nature, scope, context or purposes of the processing would be changed was developed and documented; • the respective data protection supervisory authorities were consulted if there are residual high risks which cannot be mitigated.

INTEGRATION OF DPIA OUTCOMES

Having conducted DPIA and prepared DPIA outcome report the personnel responsible for personal data protection in SBSF should:

- provide integration of the DPIA results to the project plans of the SBSF;
- identify any action points and who is responsible for implementing them (using the usual project-management process);
- monitor the ongoing performance of the DPIA;
- consult the respective data protection supervisory authority before going ahead with the processing of personal data (if it was decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high);
- publish the DPIA results with excluding all commercially sensitive information (if the respective decision on publishing such results will be taken);
- keep DPIA under review;
- repeat DPIA if there is a substantial change to the nature, scope, context or purposes of personal data processing;
- document all information related to DPIA to the Register on Collecting and Processing of Personal Data;
- provide training for relevant staff on how to carry out a DPIA.

Annex № 4

DPIA SCREENING TEMPLATE

Date: _____ **Place: _____**

CONTROLLER DETAILS

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

- **STEP 1: IDENTIFY THE NEED FOR DPIA**

what project aims to achieve and what type of processing it involves	
to refer or link to other documents, such as a project proposal	
to summarize why the SBSF identified the need for a DPIA	

- **STEP 2: DESCRIBE THE PROCESSING**

Describe the nature of the processing	
how will data be collected, used, stored and deleted?	
what is the source of the data?	
will the data be shared with anyone?	
to refer to a flow diagram or other way of describing data flows	
what types of processing identified as likely high risk are involved?	
Describe the scope of the processing	
what is the nature of the data, and does it include special category or criminal offence data?	
how much data will be collected and used?	
how often?	
how long will it be kept?	
how many individuals are affected?	
what geographical area does it cover?	
is the SBSF signed up to any approved code of conduct or certification scheme (once any have been approved)?	
Describe the context of the processing	
what is the nature of the SBSF's relationship with the individuals?	

how much control will they have?	
would they expect the SBSF to use their data in this way?	
do they include children or other vulnerable groups?	
are there prior concerns over this type of processing or security flaws?	
is it novel in any way?	
what is the current state of technology in this area?	
are there any current issues of public concern that the SBSF should factor in?	
Describe the purposes of the processing	
what do the SBSF want to achieve?	
what is the intended effect on individuals?	
what are the benefits of the processing – for the SBSF, and more broadly?	

- **STEP 3: CONSULTATION PROCESS**

Consider how to consult with relevant stakeholders	
describe when and how the SBSF will seek individuals' views – or justify why it's not appropriate to do so.	
who else do the SBSF need to involve within the SBSF?	
does the SBSF need to ask the SBSF y's processors to assist?	
do the SBSF plan to consult information security experts, or any other experts?	

- **STEP 4: ASSESS NECESSITY AND PROPORTIONALITY**

Describe compliance and proportionality measures, in particular	
what is the SBSF's lawful basis for processing?	
does the processing actually achieve the SBSF's purpose?	
is there another way to achieve the same outcome?	
how will the SBSF prevent function creep?	
how will the SBSF ensure data quality and data minimization?	
what information will the SBSF give individuals?	
how will the SBSF help to support the rights of the individuals?	
what measures does the SBSF take to ensure processors comply?	
how does the SBSF safeguard any	

international transfers?	

- **STEP 5: IDENTIFY AND ASSESS RISKS**

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

- **STEP 6: IDENTIFY MEASURES TO REDUCE RISK**

Identify additional measures the SBSF y could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

- **STEP 7: SIGN OFF AND RECORD OUTCOMES**

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the data protection specialists before going ahead
Advice provided:		Data protection specialist should advise on compliance, step 6 measures and whether processing can proceed
Summary of the advice of data protection specialists:		
The advice of data protection specialists accepted or overruled by:		If overruled, the SBSF must explain the reasons
Comments:		
Consultation responses reviewed by:		If the SBSF's decision departs from individuals' views, the SBSF must explain the reasons
Comments:		

This DPIA will kept under review by:		The representative of the respective data protection supervisory authority may also review ongoing compliance with DPIA

Annex № 5

CONSENT TO THE PROCESSING OF PERSONAL DATA

1. Template of the consent to the processing of personal data for Web-sites and Mobile Applications users.

DECLARATION ON CONSENT
PERSONAL DATA PROCESSING

This Declaration on personal data processing ("Declaration") describes how _____ as Personal Data controller and the legal entities related to SBSF (hereinafter collectively "SBSF") handles Personal Data (as defined below) and your rights with respect to processing of such Personal Data[1].

The processing of your Personal Data enables SBSF to provide you with services, charity and other help to applicants and give a proper access to the web-sites and mobile apps published by SBSF (*list of websites and Mobile Apps*), to communicate and support the applicants, following the provisions of applicable legislation.

Personal data:

- name, surname;
- e-mail;
- mobile telephone number;
- city and state.

_____ may process the Personal Data in the course of any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available[2], alignment or combination, restriction, erasure or destruction.

Hereby I also confirm on notifying me on my rights[3] exercised in relation to processing of personal data therefrom.
The period for which the Personal Data is stored is strictly limited and shall be conducted exclusively during the period necessary for the purposes mentioned above.

[1]according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);

[2] It presumes disclosure by transmission, dissemination or otherwise making available of the Personal Data to the legal entities within SBSF group of legal entities as well as the third parties, which SBSF concluded agreements with to follow the purposes of personal data processing under this consent (including foreign legal entities);

[3] Data subject is entitled to be provided with the following information: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; the fact that the controller intends to transfer personal data to a third country; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The respective requests should be sent to: privacy@bysol.org

If the consent given with signing of this Declaration is the legal basis for the processing of the Personal Data it can be withdrawn at any time[1].

Hereby I provide my consent to follow the rights and obligations mentioned in this Declaration.

Date _____
Signature _____

2. Template of the consent to the processing of personal data for Web-sites and Mobile Applications users (e-commerce).

DECLARATION ON CONSENT
PERSONAL DATA PROCESSING

This Declaration on personal data processing ("Declaration") describes how _____ as Personal Data controller and the legal entities related to SBSF (hereinafter collectively "SBSF") handles Personal Data (as defined below) and your rights with respect to processing of such Personal Data[2].

The processing of your Personal Data enables SBSF to provide you with the respective services, charity and help to give a proper access to the web-site _____ and mobile application _____, to communicate and support the applicants, following the provisions of applicable legislation.

Personal data:
- name, surname;
- e-mail;
- mobile telephone number;
- city and state;
- information on bank payment cards (name of card owner, number, validity term and CVV code).

_____ may process the Personal Data in the course of any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available[3], alignment or combination, restriction, erasure or destruction.

Hereby I also confirm on notifying me on my rights[4] exercised in relation to processing of personal data therefrom.

---

[1] This will not affect the lawfulness of the processing of the Personal Data based on such consent before the withdrawal. The consent may be withdrawn by contacting privacy@bysol.org. SBSF may be able to retain the Personal Data even if the consent is withdrawn and the Personal Data is processed on the other legal basis.
[2] according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);
[3] It presumes disclosure by transmission, dissemination or otherwise making available of the Personal Data to the legal entities within SBSF group of legal entities as well as the third parties, which SBSF concluded agreements with to follow the purposes of personal data processing under this consent (including foreign legal entities);
[4] Data subject is entitled to be provided with the following information: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the legitimate

The period for which the Personal Data is stored is strictly limited and shall be conducted exclusively during the period necessary for the purposes mentioned above.

If the consent given with signing of this Declaration is the legal basis for the processing of the Personal Data it can be withdrawn at any time[1].

Hereby I provide my consent to follow the rights and obligations mentioned in this Declaration.

Date _____
Signature _____

3. Template of the consent to the processing of personal data for for social marketing purposes.

DECLARATION ON CONSENT
PERSONAL DATA PROCESSING

This Declaration on personal data processing ("Declaration") describes how _____ as Personal Data controller and the legal entities related to SBSF (hereinafter collectively "SBSF") handles Personal Data (as defined below) and your rights with respect to processing of such Personal Data[2].

The processing of your Personal Data enables SBSF to _____.

Personal data: _____.

_____ may process the Personal Data in the course of any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available[3], alignment or combination, restriction, erasure or destruction.

---

interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; the fact that the controller intends to transfer personal data to a third country; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The respective requests should be sent to: privacy@bysol.org; [1] This will not affect the lawfulness of the processing of the Personal Data based on such consent before the withdrawal. The consent may be withdrawn by contacting privacy@bysol.org. SBSF may be able to retain the Personal Data even if the consent is withdrawn and the Personal Data is processed on the other legal basis.

[1] This will not affect the lawfulness of the processing of the Personal Data based on such consent before the withdrawal. The consent may be withdrawn by contacting privacy@bysol.org. SBSF may be able to retain the Personal Data even if the consent is withdrawn and the Personal Data is processed on the other legal basis.

[2]according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);

[3] It presumes disclosure by transmission, dissemination or otherwise making available of the Personal Data to the legal entities within SBSF group of legal entities as well as the third parties, which SBSF concluded agreements with to follow the purposes of personal data processing under this consent (including foreign legal entities);

Hereby I also confirm on notifying me on my rights[1] exercised in relation to processing of personal data therefrom.

The period for which the Personal Data is stored is strictly limited and shall be conducted exclusively during the period necessary for the purposes mentioned above.

If the consent given with signing of this Declaration is the legal basis for the processing of the Personal Data it can be withdrawn at any time[2].
Hereby I provide my consent to follow the rights and obligations mentioned in this Declaration.

Date _____
Signature _____

[1] Data subject is entitled to be provided with the following information: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; the fact that the controller intends to transfer personal data to a third country; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The respective requests should be sent to: privacy@bysol.org;

[2] This will not affect the lawfulness of the processing of the Personal Data based on such consent before the withdrawal. The consent may be withdrawn by contacting privacy@bysol.org. SBSF may be able to retain the Personal Data even if the consent is withdrawn and the Personal Data is processed on the other legal basis.

Annex № 6

CONTRACTUAL PROVISION
ON DATA PROTECTION PROCESSING

PERSONAL DATA PROTECTION

The Parties is obliged to fulfill the provision on personal data protection according to the law applicable to the Agreement. The Parties may provide specific conditions of personal data protection under the annexes to this Agreement.

In particular, the Parties are obliged to take necessary legal, organizational and technical measures for personal data protection preventing an unauthorized disclosure. Each Party is entitled to request the other Party on the legal, organizational and technical measures taken for the purposes of security of personal data processing.

Each Party is also obliged not to disclose personal data got from the other Party without the respective consent of such Party unless such obligation on disclosure is necessary for fulfillment of obligation under this Agreement or the applicable law.

The Parties ensure that personal data were duly received by them on the legal basis and for legitimate purposes.

Those individuals who sign this Agreement on behalf of the Parties provide their consent to processing of their personal data (including to transmission of such personal data abroad) for the purposes of fulfillment of the provisions of this Agreement. In case of any questions related to personal data protection the Parties agreed to request the representatives of the Parties responsible for personal data protection: _____: privacy@bysol.com, _____: _____.

Annex № 7

AGREEMENT ON
THE PROCESSING AND TRANSFER OF PERSONAL DATA

_____
_____

_____, a legal entity which is registered and operates in accordance with the laws of _____, represented by _____, acting on the basis of the _____ (the "Data exporter"),
and
_____, a legal entity which is registered and operates in accordance with the laws of Ukraine, represented by _____, acting on the basis of the _____ (the "Data importer"),
hereinafter together referred to as "the Parties", and each separately – the "Party" have concluded this Agreement in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer of the personal data specified in the Annex hereto (the "Agreement").

I. DEFINITIONS

Supervisory authority means the data protection authority in _____ (postal address: _____; email: _____).
Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data exporter means the data controller who transfers the personal data.
Data importer means the data processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions.
Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural living person.
Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject means any identified or identifiable natural person whose personal data is collected and processed by SBSF.

II. DETAILS OF THE TRANSFER

The details of the transfer and of the personal data are specified in Annex to this Agreement. The Parties may execute additional annexes to cover additional data transfers. The Parties agree that Annex to this Agreement may contain confidential activity information, which they will not disclose to third Parties, except as required by law or in response to a competent regulatory or government authority, or as required under the Agreement.

III. OBLIGATIONS OF THE DATA EXPORTER AND DATA IMPORTER

The data exporter warrants and undertakes the following:

- personal data processing, including collecting and transfer of personal data was and is conducted in accordance with the data protection laws of _____, in particular the purposes of collection of the personal data correspond in full with the purposes of transfer of personal data;
- it has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under this Agreement;
- it has instructed and throughout the duration of the personal data processing will instruct the data importer that personal data processing is possible only in accordance with the instructions of the data exporter and pursuant to the data protection laws of _____ and this Agreement;
- it will respond to requests from the data subjects and the supervisory authority concerning processing of the personal data by the data importer within a reasonable time;
- it will make available, upon request, a copy of the Agreement to the data subjects. in case the Agreement contains confidential information, it may remove such information before providing the text of the Agreement.

The data importer warrants and undertakes the following:

- it will take technical and organizational measures established under the laws of _____ of data protection against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected;
- it will have in place procedures so that any third party it authorizes to have access to the personal data will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer shall be obligated to process the personal data only on instructions from the data importer. this provision does not apply to persons authorized or required by law of _____, to have access to the personal data;
- it will process the personal data exclusively in accordance with the _____ legislation on personal data processing, this Agreement, assignments from the data exporter and for the purposes described in the Annex to this Agreement, and has the legal authority to conclude this Agreement;
- it will identify to the data exporter a contact person within its organization authorized to respond to requests concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the supervisory authority concerning all such requests within a reasonable time;
- it will process the personal data, at its option, in accordance with the data protection laws of _____;
- it will not disclose or transfer the personal data to a third party located outside _____ unless it receives approval from the data exporter about the transfer and guarantees one of the following: (1) the third party is located in a country that ensures an adequate level of personal data according to the _____ law, or (2) the third party concludes the Agreement analogous with this Agreement; or (3) with regard to onward transfers of personal data on racial or ethnic origin, political, religious or ideological beliefs, membership in political Parties and trade unions, as well as the data concerning the state of health or sexual life the data subjects have given an unambiguous consent to such transfer.

IV. LIABILITY AND THIRD PARTY RIGHTS

Each Party shall be liable to the other Party for material (financial) damages it causes by any breach of this Agreement. Liability as between the Parties is limited to actual damage suffered. Punitive damages are specifically excluded. Each Party shall be liable to data subjects for damages it causes to them as a result violation of this Agreement. This does not affect the liability of the data exporter under the legislation of _____ on personal data protection.

The Parties agree that a data subject shall have the right to enforce as a third party beneficiary this article and all other related clauses of this Agreement, against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subjects may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against the data exporter that has failed to comply with this Agreement.

V. APPLICABLE LAW

The law applied to this Agreement is the substantial law of _____.

VI. RESOLUTION OF DISPUTES WITH DATA

In the event of a dispute related the data subject or the supervisory authority concerning the processing of the personal data against either or both of the Parties, the Parties will inform each other on it, and will cooperate with a view to settling them amicably in a timely manner.

Each Party agrees and understands to perform a decision of a competent court of _____ or orders (recommendations) of the supervisory authority on eliminating the violation of legislation in the field of personal data protection

VII. TERMINATION

In the event that the data importer for the first time ever breaches its obligations under this Agreement, then the data exporter may temporarily suspend the transfer/processing of personal data to the data importer until the breach is remedied.

Data exporter has the right to terminate this Agreement in the following cases:

- the data importer is in persistent breach of any obligations given by it under this Agreement; or
- a final decision of a competent court of _____ that there has been a breach of the Agreement by the data importer is taken; or
- the data importer is subject to liquidation or an act of bankruptcy is committed.

Importer may terminate this Agreement in the following cases:

- the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month; or
- compliance by the data importer with this Agreement would put it in breach of its legal or regulatory obligations in the country of import; or
- a competent court of _____ made a final decision that there has been a breach of the Agreement by the data exporter is taken.

In case this Agreement is terminated the data importer must destroy all personal data received from the data exporter under this Agreement as well as notify all third parties, to which personal data were transferred by the data importer, on the necessity to destroy such personal data.

VIII. DETAILS OF THE PARTIES

Data exporter: Data importer:

_____ _____
_____ _____

ANNEX TO
AGREEMENT ON THE PROCESSING AND TRANSFER OF PERSONAL DATA

DETAILS ON THE PERSONAL DATA TRANSFER

DATE OF TRANSFER: _____

DATA SUBJECTS: The personal data transferred concern the following categories of the data subjects: natural persons - citizens of _____, aged 16 and older (or acquired full civil capacity under the law of _____).

CATEGORIES OF THE PERSONAL DATA: _____

PURPOSE OF THE PERSONAL DATA PROCESSING (TRANSFER): _____

THIRD PARTIES: the personal data may be transferred by the data importer only for the following third Parties (including the transfer of personal data outside _____, including to countries outside the European Economic Area, in particular to the United States of America): (1) persons affiliated with the importer; (2) to third Parties with which the contractor has entered into the relevant Agreement.

THE SENSITIVE DATA (IF APPLICABLE): n/a

DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY THE DATA IMPORTER: _____

COUNTRIES TO WHICH DATA TRANSFER WILL BE MADE: _____

TERM OF PROCESSING: __ (____) years from the signing data, if a longer period of storage is not required in accordance with the current legislation of _____.

CONTACT INFORMATION OF DATA PROTECTION OFFICERS RESPONSIBLE FOR REQUESTS CONCERNING THE PERSONAL DATA: _____

DETAILS OF THE PARTIES

DATA EXPORTER: DATA IMPORTER:

_____ _____
_____ _____

Annex № 8

DECLARATION ON CONSENT
PERSONAL DATA PROCESSING FOR CANDIDATES
WHO APPLYING FOR POSITIONS

This Declaration on personal data processing ("Declaration") describes how _____ as Personal Data controller and the legal entities related to SBSF (hereinafter collectively "SBSF") handles Personal Data (as defined below) and your rights with respect to processing of such Personal Data[1].

The processing of your Personal Data enables SBSF to review and consider your application to the vacancy announced by SBSF.

Personal data: all information inserted to the CV, namely _____.

_____ may process the Personal Data in the course of any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available[2], alignment or combination, restriction, erasure or destruction.

Hereby I also confirm on notifying me on my rights[3] exercised in relation to processing of personal data therefrom.

The period for which the Personal Data is stored is strictly limited and shall be conducted exclusively during the period necessary for the purposes mentioned above.

If the consent given with signing of this Declaration is the legal basis for the processing of the Personal Data it can be withdrawn at any time[4].

Hereby I provide my consent to follow the rights and obligations mentioned in this Declaration.

Date _____
Signature _____

[1]according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);

[2] It presumes disclosure by transmission, dissemination or otherwise making available of the Personal Data to the legal entities within SBSF group of legal entities as well as the third parties, which SBSF concluded agreements with to follow the purposes of personal data processing under this consent (including foreign legal entities);

[3] Data subject is entitled to be provided with the following information: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; the fact that the controller intends to transfer personal data to a third country; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The respective requests should be sent to: privacy@bysol.org;

[4] This will not affect the lawfulness of the processing of the Personal Data based on such consent before the withdrawal. The consent may be withdrawn by contacting privacy@bysol.org. SBSF may be able to retain the Personal Data even if the consent is withdrawn and the Personal Data is processed on the other legal basis.

Annex № 9

DECLARATION ON
CONSENT/CONTRACTUAL PROVISIONS
PERSONAL DATA PROCESSING FOR EMPLOYEES

DECLARATION ON PERSONAL DATA PROCESSING

_____
_____

This Declaration on personal data processing ("Declaration") describes how _____ as Personal Data controller and the legal entities related to SBSF (hereinafter collectively "SBSF") handles employees' (hereinafter "Personnel") Personal Data (as defined below) and your rights with respect to processing of such Personal Data.

SBSF processes the Personal Data since your employment as well as after termination of hiring for processing of the Personal Data to the extent necessary to fulfill the purposes defined under the Declaration. "Personal Data" means any information relating to an identified or identifiable natural person.

Types of Personal Data

SBSF collects and processes the following types of Personal Data about you:

1. Personal details: name, address and contact information, national identity/insurance numbers, tax identifiers, passport, date of birth, birth place, gender, immigration status and eligibility to work, photographs;
2. Family composition: marital status, name and date of birth of spouse and/or dependents and emergency contact details;
3. Career history: information provided under curriculum vitaes (CVs);
4. Education and vocational training, language, and other job-related skills;
5. Financial details, including salary, bonuses, expense reimbursement and benefit information, bank account numbers necessary for charging the respective payments;
6. Information regarding use of SBSF resources, including video surveillance footage and computer usage information (provided that the actions necessary for collecting and processing of such information were conducted by SBSF in explicit and legitimate way and in compliance with local legislation).
7. Information about health (exclusively to the extend envisaged under labour applicable legislation).

SBSF may acquire other types of Personal Data from you, from other employees or third parties. For example, SBSF may receive Personal Data from referees, recruiters, previous employers, educational establishments, colleagues and managers, applicants and activity contacts, consultants, or public sources. In this regard SBSF guarantees that such Personal Data was initially collected and received in due course and in legitimate way without any violation of your rights.

Purposes for Processing Your Personal Data

The processing of your Personal Data enables SBSF to perform its role as an employer, including fulfilling its legal obligations under applicable laws and as necessary in connection with SBSF's performance of its contractual and employment obligations to you. Without this information, it would not be possible for SBSF to perform its contract and/or legal obligations

with you. Certain Personal Data is processed by SBSF for its legitimate activity interests, including, but not limited to:

1. recruiting and employee on-boarding;
2. payroll administration;
3. pension administration;
4. health administration/health insurance/benefits;
5. expense reimbursement and management;
6. contacting others in the event of an emergency;
7. making information available within internal IT-systems and to facilitate communication between and among employees within SBSF;
8. administration and management of your access to information technology systems, including monitoring communications related and within job responsibilities executed with the labor devices in protection of SBSF property, and for investigations and disciplinary action (provided that the actions necessary for collecting and processing of such data were conducted by SBSF in explicit and legitimate way and in compliance with local legislation);
9. time entry and leave management;
10. training and appraisal, including performance records and disciplinary records;
11. employee surveys;
12. for social marketing and/or public relations purposes and in connection with the performance of your duties (e.g., SBSF may send your contact information to applicants and potential applicants as part of the social marketing so they can contact you); and
13. to comply with applicable laws and legal obligations, including without limitation:
    a. to maintain the ethics hotline;
    b. to respond to governmental inquiries or requests from public authorities;
    c. to comply with valid legal process or discovery obligations;
    d. to protect the rights, privacy, safety or property of SBSF, its workers or the public if such a disclosure is proportionate in the individual case;
    e. to permit SBSF to pursue available remedies or limit the damages that SBSF may sustain;
    f. to respond to an emergency; and/or
    g. to comply with applicable regulations, policies and procedures.

The types of Personal Data processed should correspond in full to the purposes of collection of such Personal Data each time of processing of such Personal Data.

Types of processing of Your Personal Data

SBSF may process Your Personal Data in the course of any operation or set of operations which is performed on Your Personal Data or on sets of Your Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Disclosure of Your Personal Data

SBSF may disclose and/or transfer your Personal Data to third parties (including abroad) for the purposes set out above. The parties to whom SBSF may disclose or otherwise transfer your Personal Data include:

1. legal entities related to SBSF corporation for purposes consistent with their legitimate activity practices;
2. third parties, including applicants, auditors, accountants, attorneys, and other professional advisers and third-party companies to allow SBSF to comply with contractual, statutory and other obligations, and for the proper management of its activity; and/or

3. government authorities and/or law enforcement officials if required for the purposes above, if mandated by law and if required for the legal protection of SBSF's legitimate interests in compliance with applicable laws.

International Transfers of Your Personal Data

In the course of operating its activity, SBSF may need to transfer Personal Data collected in the European Economic Area ("EEA") to countries outside the EEA which may not have laws offering the same level of protection for personal information as those inside the EEA. SBSF has taken steps to ensure adequate safeguards are adopted to protect your Personal Data. For further details of these adequate safeguards, please contact privacy@bysol.org.

Personal Data Accuracy

To ensure that the information that the SBSF maintains about you is accurate and up-to-date, please keep the SBSF informed of any changes to your Personal Data.

Security

SBSF maintains reasonable technical and organizational measures to protect your Personal Data against unauthorised or unlawful use or accidental, loss, damage or destruction.

Personal Data Retention

SBSF will store and maintain your Personal Data for the course of the employment relationship and for as long as necessary (i) for the purposes for which it was collected, (ii) to meet its current and future legal obligations, including in compliance with SBSF's records retention policy, and (iii) as permitted to meet its legitimate interests. Please note that you may have the right to request the correction or deletion of your Personal Data requesting to the address: privacy@bysol.org

Rights in relation to Your Personal Data

Subject to applicable exemptions, you have the right to:

- be informed about the Personal Data that is held about you by SBSF;
- request access to or a copy of your Personal Data that is maintained by SBSF and be provided information in relation to that data (including the purposes for which the data is processed and how long it will be stored for);
- request that your Personal Data be corrected or deleted;
- receive a copy of your Personal Data in a machine-readable format or to have your Personal Data sent to another entity;
- restrict the processing of your Personal Data;
- object to the processing of your Personal Data;
- not to be subject to a decision which is based on automated decision making or profiling that could result in a significant effect on you, such as discriminatory effects;
- withdraw the Declaration at any time provided with signing of this Declaration; and
- file a complaint with the relevant supervisory authority for violations of data protection laws.

You may make these requests by contacting SBSF at: privacy@bysol.org.

Requests with respect to these rights will be honored within 30 calendar days of the request, but (where permissible) the time period may be extended for another 2 months for complex requests.

You will be notified within 30 calendar days of the reasons for any extension.

Access to personal data may be denied in some circumstances if making the information available would reveal personal information about another person or if SBSF is legally prevented from disclosing such information.

If your consent given with signing of this Declaration is the legal basis for the processing of your Personal Data, you may withdraw your consent at any time. This will not affect the lawfulness of the processing based on your consent before the withdrawal. You can withdraw your consent by contacting privacy@bysol.org. SBSF may be able to retain data even if you withdraw your consent in case Personal Data is processed on the other legal basis.

Questions and Complaints

Please contact SBSF at privacy@bysol.org if you have questions or complaints regarding this Declaration or how SBSF processes your Personal Data. Alternatively, you may contact your local supervisory authority.

Hereby I, _____, provide my consent to follow the rights and obligations mentioned in this Declaration.

Signature _____

Date _____

Annex № 10

RESPONSE ON
THE REQUIEST OF DATA SUBJECT

Date: _____ Place: _____
(1 month from receiving request as the latest)

_____
_____
_____

Dear _____,

Pursuant to your request dated _____ please note the following:

1. Confirmation on personal data collection and/or processing

Hereby SBSF confirms that your personal data is collected and/or processed *(please choose the variant which is relevant).* In this regard data controller is: _____ *(please insert name, location and contact details),* data processor is: _____ *(please insert name, location and contact details)*.
/ Hereby SBSF confirms that your personal data is collected and/or processed *(please choose the variant which is relevant)* by _____.
/Hereby SBSF informs you that the requested information cannot be provided to you, because _____ *(it's necessary to insert a legitimate reason for such refusal).*

2. Copy of your personal data

Attached please find a set of copies containing your personal data. No extra fee is required for provision of such copies.
/ Due to the character of the request a reasonable fee should be taken (i.e. the administrative costs of providing the information or communication or taking the action requested) to the amount _____. Please pay the respective fee under the attached invoice and your request will be processed in due terms.

3. Other information

Purposes of data processing	
Categories of personal data concerned	
Third parties or categories of third parties to whom personal data disclosed	
Retention period	

You may also request rectification, erasure of personal data, restriction of processing of personal data, object to such processing as well as to lodge a complaint with a supervisory authority (_____ *(name and contact details)).*

For any details on collection and processing of your personal data please contact _____ *(name and contact details).*
_____/_____/

Annex № 11

STANDARD OPERATION PROCEDURE
ON THE MATTERS RELATED TO PERSONAL DATA BREACHES

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis, including employees, independent contractors, applicants, activity partners and other individuals SBSF dealing with.

In this regard and pursuant to Part XV of SBSF General Personal Data Protection Policy this Standard operation procedure on the matters related to personal data breaches (hereinafter – "SOP") is adopted. SOP includes provisions on breach detection, investigation and internal reporting procedures.

BREACH DETECTION

SBSF considers as data breach any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by SBSF.

Any employee of SBSF is obliged to notify the personnel responsible for personal data protection on any incident which is considered or is likely to be considered as security incident related to personal data in ___ *(period of time)* since such incident occurred or the information on such incident appeared.

SBSF shall constantly communicate with data processor. If this processor suffers a personal data breach, then it must inform SBSF on such breach without undue delay as soon as it becomes aware.

ROLE OF THE PERSONNEL RESPONSIBLE FOR DATA PROTECTION

The personnel responsible for personal data protection in SBSF are responsible for:
- preventing personal data breaches;
- detecting personal data breaches (including to take final decision on whether any incident is personal data breach or not);
- due documenting of personal data breaches;
- managing of personal data breaches;
- implementing a response plan for addressing any personal data breaches that occur;
- communicating with IT-department of SBSF for managing the effects of personal data breach;
- representing SBSF before the respective data protection authorities on the matters related to personal data breach;
- representing SBSF before the data subjects, who entitled to get information on personal data breaches;
- investigating personal data breaches;
- taking steps within internal reporting procedure related to personal data breaches;
- taking measures to mitigate the consequences of personal data breaches.

RESPONSE PLAN

- **notification of the senior management of SBSF**

The personnel responsible for personal data protection in SBSF should notify the representatives of the senior management of SBSF on any personal data breach in ____ *(period of time)* since it was decided by the personnel responsible for personal data protection in SBSF that the incident occurred is personal data breach incident.

When providing such notification the personnel responsible for personal data protection in SBSF should provide to the senior management of SBSF the following information:

At the initial stage	**After taken urgent actions (including due notification of data protection supervisory authority)**
• a description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned; • any details on personal data breach occurrence; • information on departments and employees involved in personal data breach/data processors involved in personal data breach.	• information on whether or not the personal data breach was a result of human error or a systemic issue; • a description of the likely consequences of the personal data breach; • a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects; • the complex of measures taken to make due notification of data protection supervisory authority and data subjects; • measures to bring to responsibility the employees/data processors involved in personal data breach; • measures taken to prevent the further personal data breaches.

- **notification of the data protection supervisory authority**

The obligations on notification of supervisory authority and data subject are feasible only in case such data breach occurred in those affiliated legal entity of SBSF, which is established and operate in the state with such obligations envisaged under applicable law.

As soon as SBSF becomes aware that personal data breach has occurred, it should notify respectively the supervisory authority without undue delay, but not later than 72 hours after having become aware of it, unless SBSF is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights of data subjects.

Where such notification cannot be achieved by SBSF within 72 hours, the reasons for the delay should accompany the notification conducted by SBSF further made without undue delay. Such notification should be conducted with use of the notification template attached.

When reporting a breach SBSF must provide:

- a description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Notification should be conducted even if we there are not all details on the data breach incident yet. The required information may be provided in phases, as long as this is done without undue further delay. In this regard SBSF shall file to the respective data protection supervisory authority a statement of explanation on the delay noting when SBSF expects to submit more information.
In case it is decided that the personal data breach is unlikely to result in a risk to the rights of data subjects and notification of the data protection supervisory authorities is not required the respective decision should be documented in the Register on Collecting and Processing of Personal Data.

- **notification of the data subjects**

As soon as SBSF becomes aware that personal data breach has occurred, it should also communicate to the data subject without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of data subject. Such notification should be conducted with use of the notification template attached.

When a personal data breach has occurred, SBSF need to establish the likelihood and severity of the resulting high risk to people's rights and freedoms.

When informing a breach to data subjects SBSF need to describe, in clear and plain language, the nature of the personal data breach and contain:
- the name and contact details of data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

If it is decided not to report the breach, SBSF need to justify this decision with documenting it in the Register on Collecting and Processing of Personal Data.

INVESTIGATION

The personnel responsible for data protection in SBSF should investigate the following aspects on any personal data breach occurred in SBSF:
- the details on personal data breach occurrence;
- departments and employees involved in personal data breach/data processors involved in data breach;
- whether or not the breach was a result of human error or a systemic issue;
- the complex of measures taken to make due notification of the senior management of SBSF, data protection supervisory authority, data subjects;
- measures taken to prevent the further data breaches;
- measures to bring to responsibility the employees/data processors involved in data breach.

During such investigation the personnel responsible for data protection in SBSF should be guided by the internal corporate rules on conducting investigations, if any. In addition, the personnel responsible for data protection in SBSF should cooperate with the other departments

in SBSF. The personnel responsible for data protection in SBSF are also entitled to request assistance of any third parties on the matter of data breaches in the course of investigation stage.
The results of the investigation should be documented in the Register on Collecting and Processing of Personal Data.

INTERNAL REPORTING PROCEDURES

SBSF must also keep a record of any personal data breaches, regardless of whether SBSF is required to notify.

Information on any data breaches or any related risks should be recorded to the Register on Collecting and Processing of Personal Data during 3 (three) working days after such accident took place. Such information should contain at least (1) the facts relating to the personal data breach, (2) its effects and (3) the remedial action taken.

The personal responsible for personal data protection in SBSF should during 3 (three) working days commencing data breach initiate taking of all legal, organizational and technical measures to ensure further data security.

SOP FOR PERSONNEL RESPONSIBLE FOR PERSONAL DATA PROTECTION IN CASE OF PERSONAL DATA BREACH

1. To reveal/to get information on the incident related to personal data.

2. To detect personal data breach (including to take final decision on whether any incident is personal data breach or not).

3. To determine and take an urgent set of actions to manage personal data breach, to communicate with IT-department of SBSF. If necessary to make an immediate communication with senior management of SBSF and the third parties requesting assistance to manage the incident of personal data breach.

4. To implement a response plan for addressing any personal data breaches, which occur: (1) senior management of SBSF – within ___, (2) data subjects (if necessary) – within _____, (3) respective data protection supervisory authority – within 72 hours.

5. To document the respective information on personal data breach in the Register on Collecting and Processing of Personal Data.

6. To conduct an investigation of personal data breaches occurred.

7. To take measures for bringing to responsibility the employees/data processors involved in personal data breach.

8. To develop a strategy and take a set of steps to mitigate the risk resulting of the occurred personal data breach, to communicate with IT-department of SBSF for managing the effects of personal data breach, to report the senior management the taken measures.

9. To document all respective actions taken in relation of the detected personal data breach, insert the relevant information to the Register on Collecting and Processing of Personal Data.

10. To take a set of measures to prevent further personal data breach incidents.

Annex № 12

TEMPLATE FOR NOTIFICATION
OF THE DATA PROTECTION SUPERVISORY AUTHORITY ON
PERSONAL DATA BREACH

Date: _____ Place: _____

Information on the reporting SBSF:
Name: _____.
Location: _____.
Contact: _____.

Data protection officer/personal responsible for personal data protection: _____.
Contact details: _____.

Report type:
initial report/follow-up report

Reason for report:
I consider the incident meets the threshold to report/ I do not consider the incident meets the threshold to report, however, I consider it's better to notify/I am unclear whether the incident meets the threshold to report

About the breach:
Details on the personal data breach:
- is it a result of cyber-incident?
- when did the breach happen?
- how and when did you find the breach?

Categories of personal data incurred: _____.
Number of personal data records concerned: _____.
Number of data subjects, which could be affected: _____.
Categories of data subjects, which could be affected: _____.
Potential consequences of the breach: _____.
Potential consequences of the breach for data subjects: _____.
In case the breach results from cyber incidents:
- whether confidentiality, integrity or availability of IT-system has been affected: _____.
- impact on the SBSF: _____.
- recovery time: _____.

Delay in reporting:
Yes/no

Taking actions:
Details on the actions taken or propose to take as a result of the breach.

Notification of data subjects about the breach:
Yes/no

Signature: _____

Annex № 13

TEMPLATE FOR NOTIFICATION
OF DATA SUBJECTS ON PERSONAL DATA BREACH

Date: _____ Place: _____

Information on the notifying SBSF:	Name: _____. Location: _____. Contact: _____. Data protection officer/personal responsible for personal data protection: _____. Contact details: _____.
About the breach:	Details on the personal data breach: - *is it a result of cyber-incident?* - *when did the breach happen?* - *how and when did SBSF find the breach?* Categories of personal data incurred: _____.
Description of the likely consequences of the personal data breach:	_____ _____ _____
Taking actions:	*Details on the actions taken or propose to take as a result of the breach.*

Signature: _____

Annex № 14

PERSONAL DATA RETENION POLICY

Considering privacy among the key values SBSF commits to protect personal data of all individuals involved to SBSF activity matters on a daily basis, including employees, independent contractors, applicants, activity partners and other individuals SBSF dealing with.

In this regard and pursuant to Part XIV of SBSF General Personal Data Protection Policy this Personal Data Retention Policy (hereinafter – the "Policy") is adopted.

Unless otherwise provided under the Policy or applicable law personal data may only be retained by SBSF as long as necessary for the purpose of processing.

ROLE OF THE PERSONNEL RESPONSIBLE FOR DATA PROTECTION

The personnel responsible for personal data protection in SBSF are responsible for:
- setting the retention periods for all categories of personal data collected and processed;
- reviewing and updating the retention periods for all categories of personal data collected and processed;
- controlling and managing the procedures related to personal data retention, cooperate with IT-department on these matters;
- controlling and managing the procedures related to personal data erasure/anonymization, cooperate with IT-department on these matters;
- communicating and cooperating with data protection supervisory authorities and data protection professionals on the matter related to personal data retention;
- providing responses to the requests of data subjects on personal data erasure.

PERSONAL DATA DELETION

SBSF is obliged to delete personal data in the following cases:
- data subject has withdrawn consent to processing of personal data (unless another valid legal basis has been established and communicated to the data subjects);
- contract has been performed or cannot be performed anymore and there is no need in further retention of personal data;
- personal data is no longer up to date.

SBSF shall follow the obligation mentioned above unless any obligation imposed to SBSF by law appears in this regard.

PERSONAL DATA RETENTION PERIODS

SBSF accepts such retention periods for the following processing activities:

financial and tax data for the purpose of compliance with tax regulations	for the period specified by tax laws
newsletter subscribers' information	only until consent is withdrawn by using an "unsubscribe" functionality
employee files and records	for as long as required by relevant employment and social security and social protection laws
applicant' contract, service, or	for as long as the contract is in force and the respective

delivery data	services of SBSF, charity or help are provided.

When considering the matter of expiration of the applicable retention period SBSF should take note on the information in the Register on Collecting and Processing of Personal Data.

DATA ERASURE

After the expiration of the applicable retention period SBSF should erase the respective personal data within 10 (ten) working days after such expiration. Alternatively SBSF may also take a decision on anonymization of such personal data achieved by the following means:

- erasure of the unique identifiers which allow the allocation of a data set to a unique person;
- erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
- separation of personal data from non-identifying information;
- aggregation of personal data in a way that no allocation to any individual is possible.

Information on any personal data erasure on the basis of expiration of the applicable retention period or anonymization of such personal data should be recorded to the Register on Collecting and Processing of Personal Data during 3 (three) working days after such erasure or anonymization.

REQUESTS ON PERSONAL DATA ERASURE

Data subject shall have the right to obtain from SBSF the erasure of their personal data without undue delay or restriction of processing of personal data. The personnel responsible for personal data protection should determine whether such request can be fulfilled on a case-by-case basis and provide the respective response according to the respective template.

Annex № 15

RESPONSE ON THE REQUIEST
ON ERASURE OF PERSONAL DATA

Date: _____ Place: _____
(1 month from receiving request as the latest)

_____
_____
_____

Dear _____,

Pursuant to your request dated _____ on erasure of personal data please note the following:

1. Confirmation on personal data collection and/or processing

Hereby SBSF confirms that your personal data is collected and/or processed *(please choose the variant which is relevant).* In this regard data controller is: _____ *(please insert name, location and contact details),* data processor is: _____ *(please insert name, location and contact details)*.
/ Hereby SBSF confirms that your personal data is collected and/or processed *(please choose the variant which is relevant)* by _____.
/Hereby SBSF informs you that the requested erasure of personal data cannot be conducted under your request, because _____ *(it's necessary to insert a legitimate reason for such refusal).*

2. Copy of your personal data

Attached please find a set of copies containing your personal data, which will be further erased.

Other information

	Scope of data	Date/scheduled date of data erasure
Information on data erased (live data)		
Information on data erased (backed-up data)		

/ The following categories of your personal data cannot be erased because of the following reasons:

Information on personal data out of erasure	Legal grounds for refusal in erasure of personal data	Presumed terms for personal data erasure

For any details on erasure of your personal data please contact info@bysol.org.

_____/_____/