SCIENCE & TECHNOLOGY
CENTER IN UKRAINE

STCU Standard Operating Procedure XXXIV

Data Protection

1 Purpose

This SOP establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the General Data Protection Regulation (GDPR).

The GDPR is a regulation of the European Union and the European Commission covering the data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. Therefore GDPR applies to STCU as a legal requirement where the Center collects and processes personal data of an individual resident in the EU.

STCU, as it is headquartered in Ukraine and has no registered or physical presence in the EU, does not need to follow GDPR, other than where it applies if STCU collects and processes personal data from EU citizens or residents.

As a predominately EU funded entity and to show good corporate governance as an intergovernmental organisation STCU has chosen to follow GDPR in respect of all personal data collection and processing.

2 Scope

This SOP applies to all STCU employees and all third parties responsible for the processing of personal data on behalf of STCU.

3 Policy statement

STCU is committed to conducting its operations in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This SOP sets forth the expected behaviours of STCU employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to an STCU contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. STCU, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this SOP. Non-compliance may expose STCU to complaints, regulatory action, fines and/or reputational damage. STCU, as a Data Processor is responsible for ensuring compliance with the requirements of the Data Controller and with the data protection requirements outlined in this SOP. Non-compliance may expose STCU to complaints, regulatory action, fines and/or reputational damage.

The Secretariat is fully committed to ensuring continued and effective implementation of this policy and expects all STCU employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1 Governance

3.1.1 Data protection officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, STCU has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer works with and reports to the Data Privacy Team at STCU, made up of members of the Secretariat. The Data Protection Officer's and the Data Privacy Team's duties include:

- Informing and advising STCU and its employees who carry out processing pursuant to data protection regulations, national law or EU based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or EU based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs because of STCU's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs because of STCU's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing the Secretariat and Governing Board of STCU of any potential corporate, civil and criminal penalties which may be levied against STCU and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this SOP by any third party who:

- provides personal data to STCU;
- receives personal data from STCU;
- has access to personal data collected or processed by STCU.

STCU does not in the normal course of its activities receive personal data from third parties, but from the individual themselves STCU does not in the normal course of its activities provide personal data to third parties or allow third parties access to personal data collected by STCU.

3.1.2 Data protection by design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes or services and/or when reviewing or expanding existing systems or processes or services, each of them must go through an approval process before continuing. STCU staff must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Data Privacy Team for review and approval. Where applicable, the any third-party Information Technology (IT) contractors, as part of STCU's IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

3.1.3 Compliance monitoring

To confirm that an adequate level of compliance that is being achieved by STCU in relation to this SOP, the Data Protection Officer will carry out data protection monitoring for all such services/entities either annually or as the need arises. Monitoring will, as a minimum, assess:

- Compliance with this SOP in relation to the protection of personal data, including:
- The assignment of responsibilities:
  - ✓ Raising awareness;
  - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ✓ Data subject rights;
  - ✓ Personal data transfers;
  - ✓ Personal data incident management;
  - ✓ Personal data complaints handling;
  - ✓ The level of understanding of data protection policies and privacy notices;
  - ✓ The currency of data protection policies and privacy notices;
  - ✓ The accuracy of personal data being stored;
  - ✓ The conformity of data processor activities;
  - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches.

The Data Protection Officer, in cooperation with Data Privacy Team, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the STCU Data Privacy Team.

3.2 Data protection principles

STCU has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, STCU must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means STCU must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means STCU must not store any personal data beyond what is strictly required.

Principle 4: Accuracy Personal data shall be accurate and, kept up to date. This means STCU must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means STCU must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. STCU must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability A Data Controller shall be responsible for and be able to demonstrate compliance. This means STCU must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3 Data collection

3.3.1 Data sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies (e.g. job references);
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means;
- The information must remain confidential due to a professional secrecy obligation;
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data;
- At the time of first communication if used for communication with the data subject;
- At the time of disclosure if disclosed to another recipient.

3.3.2 Data subject consent

STCU will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, STCU is committed to seeking such consent. The Data Protection Officer, in cooperation with other STCU staff, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3 Data subject notification

STCU will, when required by applicable law or contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent.

The disclosures may be given electronically or in writing. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4 External privacy notices

Any website provided by STCU will include an online ‘Privacy Policy’ and an online ‘Cookie Banner’ fulfilling the requirements of applicable law.

3.4 Data use

3.4.1 Data processing

STCU uses the personal data of its contacts for the following broad purposes:

- The operations and administration of STCU;
- To provide services to STCU’s funding parties and partners.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by STCU to respond to a contact request for information about the Center's activities. However, it will not be within their reasonable expectations that STCU would then provide their details to third parties for marketing purposes. STCU does not provide personal data to third parties for marketing purposes.

STCU will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, STCU will not process personal data unless at least one of the following requirements are met:

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a **legal obligation** to which the Data Controller 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 the Data Controller.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the Data Controller/Processor or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, STCU will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.

- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

3.4.2 Special categories of data

STCU will only process special categories of data (also known as sensitive data) where the data subject **expressly consents** to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject;
- The processing is necessary for the establishment, exercise or defence of legal claims;
- The processing is specifically authorised or required by law;
- The processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where, special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, STCU will adopt additional protection measures.

3.4.3 Children's data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

In the normal course of STCU's activities the only personal data collected from children would be in relation to the inclusion of the children of STCU staff and former staff in the medical insurance scheme.

3.4.4 Data quality

STCU will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by STCU to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification;
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period;
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required;

- Restriction, rather than deletion of personal data, insofar as:
  - ✓ a law prohibits erasure;
  - ✓ erasure would impair legitimate interests of the data subject;
  - ✓ the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.5 Profiling & automated decision making

STCU will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where STCU utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Object to the automated decision-making being carried out. STCU must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

STCU in the normal course of its activities does not carry out profiling of individuals and does not use automated decision making processes.

3.4.6 Digital marketing

As a rule, STCU does not use digital marketing in the normal course of its activities. Should there be a change in this regard STCU will not send promotional or direct marketing material to an STCU contact through digital channels such as mobile phones, e-mail and the Internet, without first obtaining their consent. STCU would not carry out a digital marketing campaign without obtaining prior Consent from the data subject. Where **personal data** (e.g. case studies or photographs) processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately, and their details should be kept on ***a suppression list*** with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5 Data retention

To ensure fair processing, personal data will not be retained by STCU for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which STCU services/entities need to retain personal data is set out in STCU's ***Data Retention Schedule*** *(Appendix A)* and in SOP XXX - Archives . This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6 Data protection

STCU will adopt physical, technical, and organisational measures to ensure the security of personal data. These measures are contained in SOP XXVIII - Information and Technology Policies and Procedures. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed;
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations;
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation;
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system;
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller;
- Ensure that personal data is protected against undesired destruction or loss;
- Ensure that personal data collected for different purposes can and is processed separately;
- Ensure that personal data is not kept longer than necessary.

3.7 Data subject requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access;
- Objection to processing;
- Objection to automated decision-making and profiling;
- Restriction of processing;
- Data portability;
- Data rectification;
- Data erasure.

If an individual makes a request relating to any of the rights listed above STCU will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. data subjects are entitled to obtain, based upon a request made in writing/e-mail to: **the Chief Administrative Officer.**

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in STCU's ***Data Subject Access Rights Policy and Procedure*** document.

3.8 Law enforcement requests & disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If STCU processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If STCU receives a request from a court or any regulatory or law enforcement authority for information relating to an STCU contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9 Data protection training

All STCU employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, STCU will receive regular Data Protection training and procedural guidance.

3.10 Data transfers

STCU may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. STCU may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.

- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.11 Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12 Breach reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail, by calling. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant STCU ‘***Data Breach Policy and Procedure’*** based on the criticality and quantity of the personal data involved. For severe personal data breaches, STCU’s Data Privacy Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

4 Roles and responsibilities

4.1 Implementation

The Secretariat and staff of STCU must ensure that all STCU employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, STCU will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by STCU.

4.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Chief Administrative Officer.

5 Review

This policy will be reviewed by the Data Protection Officer/Data Privacy Team every **three years**, unless there are any changes to regulations or legislation that would enable a review earlier.

6 Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised STCU recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of **5 years**.

7 Terms and definitions

General Data Protection Regulation (GDPR): The General Data Protection Regulation (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8 Related legislation and documents

- 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)

9 Feedback and suggestions

STCU employees may provide feedback and suggestions about this document to the Chief Administrative Officer.

10 Effectivity:

This procedure is effective 1 September 2020

Curtis Bjelajac Executive Director

Appendix A – Data Retention Schedule

Personal data record category	Mandated retention period	Record owner
Financial Records		
Financial documents	See archives policy	Finance
Financial statements	Permanent	Finance
Statutory and Governing Board		
Agreement Statute, Financial Regulations, etc	Permanent	Finance
Board documents	Permanent	Finance
Board meeting minutes	Permanent	Finance
HR: Employee Records		
Employee Records	Duration of employment and/or to provide references in the future	HR
Contracts		
Signed	Permanent	Admin
Contract amendments	Permanent	Admin
Successful tender documents	Permanent	Admin
Unsuccessful tenders' documents	Permanent	Admin
Conference, workshop and seminar documents		
Individual attendees registration documents	Cleared after the conclusion of the event	Organiser of the event