INTERNATIONAL COUNCIL FOR OPEN AND DISTANCE EDUCATION

DATA PROTECTION POLICY

GDPR for ICDE 2022 - 2024

Editor: ***Ola Eloranta, Data Protection Officer, ICDE***

Published in 2022 by the International Council for Open and Distance Education
Pløens gate 2B
0181 Oslo, Norway

TABLE OF CONTENTS

1.0 PREAMBLE

1.1 ABOUT THE GDPR

The aim of the GDPR (**G**eneral **D**ata **P**rotection **R**egulation) is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. The GDPR applies to all organisations processing the personal data of data subjects residing in the European Union, regardless of the company's location (so-called extraterritorial applicability). ICDEs activities fall within this scope.

1.2 DEFINITIONS

Personal data is defined as any information related to a natural person or "Data Subject", that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an e-mail address, bank details, posts on social networking websites, or a computer IP address.

1.3 IMPLICATIONS FOR ICDE

ICDE has in this regard implemented the below procedures in order to comply with the GDPR. It is important that all current and future ICDE Secretariat staff have sufficient knowledge about the regulation and actively ensure compliance in the day-to-day operation of the Secretariat.

2.0 DATA SUBJECT CONSENT

2.1 CONSENT UNDER THE GDPR

All obtainment of personal data from members and non-members of ICDE necessitates active consent from the data subjects.

This applies to all forms of obtainment of data, either it is through an open call advertised in a newsletter, or a webinar registration form via Squarespace or Google Docs. The request for consent must be given in an intelligible and easily accessible way, with the actual purpose of the data processing attached to the specific request for consent. It must also be as easy to withdraw consent as it is to give.

2.2 ICDE POLICY FOR OBTAINING DATA SUBJECT CONSENT

As such, this following text must be included in all communication and forms when requesting personal data about natural persons:

***

"By submitting this personal information, you agree that ICDE may process and store this data in relation to the facilitation of this specific [webinar, conference, call, application, newsletter, project, event, etc.]. To withdraw this consent, contact ICDE by e-mail at icde@icde.org and your data will be permanently deleted."

***

In the event that a data subject withdraws consent – his/her personal data shall be removed from the relevant database(s) within three (3) weeks. The Data Protection Officer is responsible for the removal – and shall confirm to the data subject when this is completed.

3.0 NOTIFICATION OF DATA BREACH

3.1 REQUIREMENTS REGARDING DATA BREACHES

Under the GDPR, organisations processing personal data must develop internal procedures for discovering and informing data subjects of data breaches. The general requirement is that information must be provided within 72 hours of first having become aware of the breach.

3.2 ICDE POLICY FOR DISCOVERING DATA BREACHES

ICDEs main tool for discovering data breaches is through the layered security systems integrated within the IT service providers. If a staff member receives an e-mail stating either that (1) a login has occurred, or that (2) a reset password request was received – and that staff member was not involved in either – it is likely that someone is trying to gain access to ICDEs systems illegitimately. In case this occurs, the staff member should immediately change his/hers/its password on the applicable service – and without undue delay inform the Data Protection Officer.

The Data Protection Officer is furthermore responsible for monitoring login activity in order to discover anomalies in the use of ICDEs services. He/she/it shall follow up accordingly and conduct inquiries when necessary. This applies to the following ICDE databases which store personal information of data subjects: Microsoft Office, 24 Seven Office, Google Drive, MailChimp, Zoom, Canva, Stripe, Squarespace, Asana, Election Runner, DocuSign, and WordPress.

3.3 ICDE POLICY FOR INFORMING ON DATA BREACHES

In the case that the Data Protection Officer on the basis of his/hers/its inquiry finds it probable that there has been a data breach – the Secretary General shall be informed without undue delay. The Secretary General shall then within 72 hours inform the relevant data subjects by e-mail of the breach and its possible extent.

4.0 RIGHT OF ACCESS

4.1 DATA SUBJECT'S RIGHT OF ACCESS TO STORED DATA

Under the GDPR, the data subjects have a right to obtain confirmation as to whether or not personal data concerning the subject is being processed, where and for what purpose.

4.2 ICDE POLICY ON THE RIGHT OF ACCESS

If ICDE receives a request regarding "if, why and/or in what way" data is processed, the receiving staff member shall conduct a search in the ICDE databases listed below. Based on what database the requesting individual appears in – the following information shall be provided within reasonable time:

ICDE Database	Location	Processing	Purpose
Microsoft Office	Cloud (European Union)	Stored=Yes	Membership Facilitation
Zoom	Cloud (Germany)	Stored=Yes	Webinar and Meetings
Stripe	Cloud (United Kingdom)	Stored=Yes	Accounting and Payments
24Seven Office	Cloud (Norway)	Stored=Yes	Membership, Accounting and Invoicing
Google Drive	Cloud (Ireland/Belgium/Denmark/Finland/ Netherlands)	Stored=Yes	Membership Facilitation and Registration
MailChimp	Cloud (USA)	Stored=Yes	Information and Communication
SquareSpace	Cloud (USA)	Stored=Yes	Membership Facilitation and Payments
Election Runner	Cloud (USA)	Stored=Yes	Voting
Canva	Cloud (USA)	Stored=Yes	Information and Communication
WordPress	Cloud (Netherlands/UK/Germany)	Stored=Yes	Project Facilitation
Asana	Cloud (Germany)	Stored=Yes	Work Task management
DNB	Cloud (Norway)	Stored=Yes	Bank, Insurance and Pension
DocuSign	Cloud (Germany/Netherlands)	Stored=Yes	Board Documentation

If the search of the requesting individual, by e-mail address, name or other relevant identifiers, does not render any result – ICDE does not process any data regarding the

individual and he/she/it may be informed of this. Data pertaining other data subjects than the requester shall not be distributed without express consent of the rightful subject.

The main reason for ICDEs processing of personal data is tied to the operation of the organisation. ICDE is a membership organisation which entails that registries containing personal data pertaining members, contacts, other affiliated natural persons and/or entities, prospective and potential members, as well as newsletter subscribers, must be stored and processed in order for ICDE to carry out is mandated work as set forth in its constitution.

5.0 RIGHT TO BE FORGOTTEN

5.1 DATA SUBJECT'S RIGHT TO BE FORGOTTEN

In order to safeguard the right to be forgotten under the GDPR, data subjects may request that their personal data is deleted from ICDEs databases. In addition, ICDE must delete personal data that is no longer relevant to the purposes of processing the data – i.e. webinar attendance lists and/or payment registration sheets that are no longer used.

5.2 ICDE POLICY ON THE RIGHT TO BE FORGOTTEN

When ICDE receives a request to delete all personal data from a specific data subject, or consent is withdrawn, the Data Protection Officer shall conduct the following actions:

ICDE Database	Action
Microsoft Office	Delete all e-mails from and to the data subject in question, as well as deletion of the entry from the contact database.
Zoom	Delete appropriate entries.
Stripe	Delete all personal data on the data subject, and all orders pertaining to the subject if the archiving time limit is reached.
24Seven Office	Delete the relevant entry in the "Customer Database" and from the "Contacts Database".
Google Drive	Search Google Drive for the data subject's information and delete appropriate documents pertaining to the subject.
MailChimp	Delete appropriate entries and the data subject's information from the Mailing lists.
SquareSpace	Delete appropriate entries and information pertaining to the data subject from the website www.icde.org
Election Runner	Delete appropriate entries.
Canva	Delete appropriate entries.
WordPress	Delete appropriate entries and information pertaining to the data subject from the website www.encoreproject.eu
Asana	Delete appropriate entries.
DNB	Delete appropriate entries which are not covered by laws of storage.
DocuSign	Delete appropriate entries.

The deletion shall be conducted without undue delay. A confirmation of the deletion shall be issued to the requesting data subject.

Personal data which the consented purpose of processing is no longer present, is also to be deleted according to the table above without undue delay and at the latest one (1) year after the purpose of obtainment ceased to exist.

6.0 DATA PORTABILITY

6.1 DATA SUBJECT'S RIGHT TO OBTAIN DATA IN A PORTABLE FORMAT

Under the GDPR, data subjects may request that the stored personal data is made available to them in a portable format.

6.2 ICDE POLICY ON DATA PORTABILITY

Upon request, ICDE shall export all the data pertaining to the data subject to a digital sheet (.csv or .xlsx) and send this to the requesting individual. The following data shall be exported and compiled:

ICDE Database	Action
Microsoft Office	If applicable, e-mail addresses and the information contained in the signature.
Zoom	If applicable, full export of the relevant contact attributes.
Stripe	If applicable, full export of the relevant payment and contact attributes.
24Seven Office	If applicable, full export of the relevant contact attributes.
Google Drive	If applicable, all additional information (such as historic membership data) of relevance pertaining to the subject.
MailChimp	If applicable, full export of the subject's subscriptions and relevant contact attributes.
SquareSpace	If applicable, full export of the relevant contact attributes.
Election Runner	If applicable, full export of the relevant contact attributes.
Canva	If applicable, full export of content pertaining to the subject.
WordPress	If applicable, full export of the relevant contact attributes.
Asana	If applicable, full export of the relevant contact attributes.
DNB	If applicable, full export of the relevant contact attributes.

The data shall be sourced and provided to the requesting individual without undue delay. A note that data was collected and delivered to the data subject shall be added to the individual's registry profile in the 24Seven Office database.

7.0 RESTRICTION OF ACCESS AND PRIVACY BY DESIGN

7.1 DATABASE ACCESS TO BE BASED ON SCOPE OF RESPONSIBILITY

In order to comply with the "Privacy by Design", ICDE has implemented a diversified access scheme as to what members of staff have access to what database. A record is also kept as to what files are accessed by whom and at what time. This is to discover activity anomalies pertaining to the access to personal information stored in the ICDE databases. The overarching goal is to ensure that the personal information only is accessed on a need-to-know basis.

7.2 ICDE POLICY ON DATABASE ACCESS

This table outlines what database is to be accessible for what Secretariat Staff, based on the individual areas of responsibility and daily tasks:

ICDE Database	Access Policy
Microsoft Office – icde@icde.org	All staff
Zoom	All staff
Stripe	Secretary General, and Communication and Administration Officer.
24Seven Office	All staff have access to the CRM and Busy (time registration). Secretary General, Communication and Administration Officer, and Accountants have access to all other services.
Google Drive	All staff have access to the ICDE Team Drive and project folders. Secretary General and Communication and Administration Officer have access to Management and Finance folder.
MailChimp	All staff
SquareSpace	All staff
Election Runner	Secretary General, Senior Advisor for Events and Projects, and Communication and Administration Officer.
Canva	All staff.
WordPress	Project Manager, and Communication and Administration Officer.
Asana	All staff.
DNB	Secretary General and Communication and Administration Officer.
DocuSign	Secretary General and Senior Advisor for Events and Projects.

Due to the size of the Secretariat and the nature of work tasks, all staff need to access a majority of ICDEs databases and tools. When reorganising work tasks and/or responsibilities – consideration should be taken whether or not to amend the distribution of access.

The ICDE Secretary General may at any time reasonably amend the above distribution of access. In case of such amendment, this policy shall without undue delay be updated accordingly.

8.0 HISTORIC DATA

8.1 HISTORIC DATA

The rules of the obtainment of consent correspondingly applies to data originating from ICDEs historic database registries. Active consent is therefore required also for the data previously obtained.

Currently, ICDEs databases contain over 20.000 entries, of which a majority originates prior to the entry into force of the GDPR. In connection with the entry into force of the GDPR in 2018, the ICDE Secretariat issued a letter to all individuals registered in its databases providing the opportunity to withdraw consent of data processing. It is therefore considered that the individuals having provided personal data prior to the entry into force of the GDPR are (i) aware of ICDEs processing of their personal data, and (ii) their rights as data subjects under the GDPR.

In the wake of dispatching the letters, ICDE further deleted historic data that it no longer had reasons to store and process. In relation to the entry into force of this revision of ICDEs GDPR Policy, a structured assessment of the compliance of all relevant historic data was made, concluding that ICDE processing of such data is compliant with the GDPR.

9.0 CYBER SECURITY AND DATA PROTECTION OFFICER

9.1 ICDE PASSWORD POLICY

In relation to the "Privacy by Design" principles, the ICDE Secretariat shall adopt the following password policy for registries falling within the scope of the GDPR:

a) Passwords shall be minimum 8 characters of length
b) Passwords shall contain minimum 1 special character (!?# etc.)
c) Passwords shall contain minimum 1 capital letter
d) Passwords shall be changed every year.

This includes, but is not limited to, the following databases: Zoom, Stripe, 24Seven Office, Google Drive, MailChimp, SquareSpace, Election Runner, Canva, Wordpress, DocuSign, and Asana.

9.2 SPAM/PHISHING E-MAILS

ICDE Secretariat staff shall also be especially aware of spam and phishing e-mails. Such e-mails shall be reported immediately to the Proofpoint spam filter, monitored and managed by ICDEs IT provider PowerIT AS. Upon reporting, all spam and phishing e-mails shall followingly be deleted immediately. All ICDE computers shall furthermore be equipped with a firewall and anti-virus software.

9.3 DATA PROTECTION OFFICER

The ICDE Secretary General shall appoint a Data Protection Officer who in addition to his/hers daily tasks, shall assume the administrative responsibilities set forth in this policy. In the absence of a Data Protection Officer, the Secretary General is responsible.

9.4 PHYSICAL COPIES AND DISPOSAL OF PAPER SHEETS

When disposing of physical copies containing personal data pertaining to the scope of the GDPR, the paper sheets shall be torn or otherwise be rendered unreadable for third parties before they are removed from the office premises.

10.0 IMPLEMENTATION OF THE POLICY

This Policy was implemented on 24 May 2018 and approved by the ICDE Secretary General. The most recent revision was carried out on 23 May 2022.

In relation to this, the sub-menu item for the "ICDE Data Privacy Policy" shall be updated on the ICDE website, where this revised Policy is available (.pdf) together with a brief outline of the rights and contact options for the data subjects.

All e-mails received by the ICDE Secretariat of GDPR relevance shall be prioritised and be acted upon without undue delay. The appointed Data Protection Officer shall be copied in on all GDPR related matters.

11.0 APPLICABILITY AND REVISION

This revised Policy shall be included in the "Welcome package" to new ICDE staff members and be circulated to all current staff. It shall also be annexed in the HMS Handbook.

This Policy is subject to bi-annual revision.

DRAFTED BY: OE, 23 May 2022
CLEARED BY: TG, 24 May 2022
APPROVED BY: TG, 24 May 2022

ICDE - International Council for Open and Distance Education,
Pløens gate 2B,
0181 Oslo, Norway

Email: icde@icde.org
Telephone: +47 22 06 26 32
Enterprise Registry Number: NO971286512