General Data Protection Regulation Policy

Procedural Information
Prepared by: Jonathan Salk, Executive Director, CORFAC International
Approved by Board/Management on: May 25, 2018
Effective Date: May 25, 2018
Annual Review Date: May 25

Forward
The essence of the General Data Protection Regulation (GDPR) is that we, as employees of CORFAC International, will not take electronic collection, transfer, storage and use of personal data of others lightly. As an organization, we are mindful and protective of our member information.

What is Our Responsibility?
As CORFAC employees, we think first about what we absolutely need from personal data. Then, only collect and use what is necessary. We will clearly get permission and assess our need to collect or use personal data. A person giving permission to use their data will be told why we need the data and be asked to say yes. We will not recycle the use of personal data for new and different purposes. We are prepared to explain and justify verbally and in writing why and what we've done. We safely keep and protect data we possess and properly discard when finished or when asked.

Introduction
CORFAC is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with our legal obligations. This policy only applies where legally required. Otherwise, requirements are voluntary by CORFAC and no legal liability or obligations are assumed. No defenses are waived.

CORFAC holds personal data about current and past employees, members, member company employees, sponsor representatives, exhibitor representatives, speakers, presenters, conference and event registrants, volunteers, service provider representatives and other individuals for a variety of business purposes.

This policy sets out how CORFAC protects personal data and outlines staff's role in following the rules governing the collection and use of personal data in the workplace. This policy requires staff to ensure that the CORFAC Executive Director is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions
CORFAC. Corporate Facility Advisors Inc.
GDPR. European Union General Data Protection Regulation.
DIT. Director of Information Technology.
DPO. A Data Protection Officer required to be appointed under the law by many but not all organizations that control or process data. The DPO operates as an auditor with regard to personal data collection and use. The DPO should have no duties which conflict with the monitoring obligations of GDPR. The DPO may be a member of staff or an outside professional knowledgeable in the field of data security and privacy.

Business Purposes. The purposes for which personal data may be used by CORFAC such as for personnel, administrative, financial, regulatory, payroll, operational, fundraising, marketing, legal and business development. Business purposes include but are not limited to:

- Compliance with legal and corporate governance obligations
- Gathering information for legal proceedings or requests and responding to subpoenas
- Operational reasons like recording transactions, accounting, preparing reports or due diligence
- Investigating complaints
- Human resources and benefits administration
- Obtaining insurance and processing claims

- Facilitating networking
- Monitoring staff conduct and disciplinary matters
- Security
- Marketing association business
- Providing member services
- Providing usage reports
- Administering continuing education
- Delivering content
- Communications
- Operating live and virtual meetings, sessions, conferences and expos
- Providing live and electronic networking opportunities
- Verifying hotel obligations
- Improving services

Personal Data. 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, by reference to an identifier such as a name, an identification number, location data, on line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include an individual's phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, licenses, business affiliations, information preferences and CV.

Special Categories of Personal Data. Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offenses or related proceedings and genetic and biometric information.

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

Processing. 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 Minimization. Limiting data collection, storage and processing to that which is adequate, relevant and necessary to successfully accomplish a task with a legitimate business purpose.

Pseudonymization. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information (e.g. a key). Such additional information must be kept separately and subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Supervisory Authority. This is the national body responsible for data protection. The supervisory authority for a U.S. based company doing business almost entirely in the U.S. is determined by laws outside of the U.S. and depends on the facts.

Scope
This policy applies to all CORFAC staff and each staff person must be familiar with this policy and comply with its terms. This policy supplements other CORFAC policies relating to internet, data protection, email use and privacy. CORFAC may supplement or amend this policy with additional policies and guidelines from time to time. New or modified policies will be circulated to staff after, upon or prior to formal adoption. The GDPR rules are not applicable to personal or household activity or to data for deceased persons. The rules apply to processing in the European Union which, for a U.S.-based association with no established Union presence, can mean processing done by outside contractors that have operations making the contractor "established in the Union," or the processing or controlling of data for subjects who are in the Union (i.e. physically overseas) by a U.S.-based association.

Oversight
CORFAC's Executive Director has overall responsibility for the day-to-day implementation of this policy. You should contact the Executive Director for further information about this policy. Please refer to the company directory for contact information for the Executive Director identified in this policy.

In addition to the Executive Director, law requires certain organizations to appoint a Data Protection Officer (DPO) to carry out mandatory tasks. CORFAC does not likely carry on operations defined in the GDPR as indicative of a need for a DPO, such as carrying-on operations (1) as a public authority, (2) that comprise a nature and scope requiring large scale monitoring or (3) that comprise large scale processing of specialized data. Therefore, CORFAC need not appoint a DPO. Nonetheless, CORFAC voluntarily appoints the CORFAC Executive Director as the Data Protection Officer for the Association to carefully monitor and oversee member data.

Unless it is obvious that an organization is not required to designate a DPO, the WP29 (an official GDPR advisory group) recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. This analysis is part of the documentation under the accountability principle. It may be required by the supervisory authority and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services that might fall within the cases listed in other portions of the law. When an organization designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to their designation, position and tasks as if the designation had been mandatory. The GDPR operates, in essence, as an auditor of an organization's data processing related activities. Where an Association does not appoint a DPO and one is not required by law, the Executive Directors and his assigns may audit operations on a voluntary basis.

Principles
CORFAC shall comply with the principles of data protection (the Principles) enumerated in the GDPR to the extent required by law. The Principles are:

1. **Lawful, fair and transparent**. Data processing must and will be fair, lawful and transparent to the person sharing their data as to how their data will be used.
2. **Limited for its purpose**. Data can only be collected for a specified, explicit, legitimate purpose and may not be repurposed for an inconsistent purpose.
3. **Acceptable further processing.** Further processing of legitimate data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the initial purposes and is acceptable by law.
4. **Data minimization.** Any data collection and processing must be relevant and limited to what is necessary.
5. **Accurate**. Data should be kept up to date where necessary. Inaccurate data must be erased or corrected.
6. **Retention**. Data in a form that identifies a person may not be kept longer than necessary.
7. **Integrity and confidentiality**. Personal data must be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Accountability and Transparency
CORFAC must and will ensure accountability and transparency in all use of personal data. CORFAC must and will be able to show authorities how staff complies with each Principle. Therefore, CORFAC staff members are responsible for keeping a written record of how all data processing activities comply with each of the Principles. Responsibility for creating and maintaining the records lies with the staff member who requests, collects or uses personal data. Written compliance records must be kept up-to-date and must be approved by the Executive Director

and DPO where a DPO has been appointed. The Executive Director shall establish and maintain the system for record keeping. To comply with data protection laws and the accountability and transparency Principle of GDPR, CORFAC must demonstrate compliance. Each staff member is responsible for understanding their responsibilities to ensure CORFAC meets the following data protection obligations:

- Fully implement all appropriate technical and organizational measures
- Maintain up-to-date and relevant documentation on all processing activities
- Conduct Data Protection Impact Assessments where appropriate
- Implement measures to ensure privacy by design and default, including:
  - Pseudonymization
  - Transparency
  - Necessity of processing
  - Allowing individuals to obtain confirmation and information regarding processing their data
  - Creating and improving security and enhanced privacy procedures on an ongoing basis

Written Records Exception

The law requires written records be kept of all processing activity. However, the law provides an exception to this requirement where CORFAC, being a small employer, defined as having less than 250 employees, conducts occasional non-risky processing where data is not within any specially protected category. Staff should consult with the Executive Director and obtain approval prior to relying on the written records exception. The conservative approach is to not rely upon the exception.

Procedures

Fair and Lawful Processing

CORFAC must and will process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This means that where consent is the legal justification for collecting data, for example, CORFAC should and will not process personal data unless the individual whose details are being processed has demonstrably and uncontrovertibly consented to the processing. In many other contexts, such as for human resources or providing member services pursuant to contract, the justifiable basis would likely be due to needs related to fulfillment of contractual obligations or pursuant to documented legitimate CORFAC interests, and these justifications should and will be made known to the person providing their information. If CORFAC cannot prove that it established a "lawful basis" to collect and process data as defined in the GDPR, processing could be deemed unlawful. Data subjects have the right to have any unlawfully processed data erased.

Registered Agent

As an organization outside the European Union and with no establishment in the European Union, CORFAC does not have and is not required to have a "registered agent" because of the express exception for occasional, less than large scale, low risk processing. In addition, with regard to possible registration with the Information Commissioners Office (ICO), CORFAC as a not-for-profit with limited activities, falls within the registration exception.

Controlling vs. Processing Data

CORFAC can likely be classified as a "data controller" and a "data processor" under the GDPR. As a data processor, CORFAC must comply with its contractual obligations and act only on the documented instructions of the data controller. If CORFAC at any point determines the purpose and means of processing without the instructions of the controller, it shall be considered a data controller and therefore breach its contract with the controller and have the same liability as the controller. As a data processor, CORFAC must:

- Not use a sub-processor without written authorization of the data controller
- Cooperate fully with a supervisory authority having jurisdiction
- Ensure the security of the processing
- Keep accurate records, where required by law, of processing activities
- Notify the controller of any personal data breaches within 72 hours
- Notify data subjects of breaches

Lawful Basis for Processing Data

CORFAC must establish a lawful basis for processing data. Each staff person must and will ensure that any data that they are responsible for managing has a written lawful basis approved by the Executive Director or DPO, where appointed, and a proper recording is made in an auditable resource identified by the Executive Director. It is each staff member's responsibility to check the lawful basis for any data they are working with and ensure all of their actions comply with the GDPR. At least one of the following justifications must apply whenever CORFAC processes personal data:

1. **Consent.** CORFAC holds demonstrable, relevant, informed, unrevoked and knowing consent from the individual who provided their data for the individual's data to be processed for the specific purpose; or
2. **Contract.** The 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; or
3. **Legal obligation.** CORFAC has a legal obligation to process the data (excluding a contract); or
4. **Vital interests.** Processing the data is necessary to protect a person's life or in a medical situation; or
5. **Public function.** Processing the data is necessary to carry out a public function, a task of public interest or the function has a clear basis in law; or
6. **Legitimate interest.** The processing is necessary for the CORFAC's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Justification based on items 2 through 6 warrant extra scrutiny regarding safeguards, consequences and original purposes of data collection as it relates to new processing.

Choosing a Lawful Basis

When making an assessment of the lawful basis, each staff member must and will first establish that the processing is necessary. This means that the processing must be a targeted, appropriate way of achieving a stated purpose. Note that staff's reliance upon a lawful basis could be deemed void and improper if the staff could have reasonably achieved the same business purpose by some other means. Therefore, necessity is primary. More than one basis may apply and staff should rely on what will best fit the purpose, not what is easiest.

Consider the following listed factors and document the answers.

General Considerations

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Does CORFAC truly need to process the data?

When Comparing Legitimate Interest vs. Consent

- Is the collection and processing for purely marketing and sales for which "consent" seems more likely as appropriate?
- Is the collection or processing needed to serve a client or customer as they expect, which tends to show "legitimate interest?"
- Would individuals expect this processing to take place? If so, this would be important as support for "legitimate interest?"
- Is access to quality news content, for example, contingent on agreeing to accept third-party advertising? If so, legitimate interest rather than consent would likely be the better choice for legal basis.
- Is CORFAC in a position of power over the data subject which might make "consent" illusory and an indefensible justification?
- Would the data subject be likely to object to the processing?
- Is CORFAC able (meaning it won't impact normal business operations such as providing benefits to an employee) to stop processing at any time on request, which could be required if "consent" is the basis?

When Considering Consent

- Consent notice must be prominent and separate from boilerplate terms and conditions
- Users must positively opt-in
- Pre-ticked boxes or any other type of default consent mechanisms are unacceptable
- Notice must be in clear, plain language that is easy to understand

- Notice must specify why CORFAC wants the data and what we're going to do with it
- Consent options should be individual ('granular') options to consent separately to different purposes and types of processing
- Notice includes the CORFAC name and third-party controllers who'll be relying on the consent
- Notice must advise individuals that they can withdraw their consent
- Individuals can refuse to consent without detriment
- Consent is not a precondition of unrelated services

For most online marketing messages, marketing calls, online tracking methods including the use of cookies, apps or other software, consent is likely required. Otherwise, alternative legal basis will likely be more appropriate. Employment and human resources materials will frequently be based on contract or legitimate interest. Processing credit cards for registrations, membership, sponsorship and booth fees are based in contract.

A commitment to the first Principle requires that CORFAC document this evaluation process and show that staff considered which lawful basis best applies to each processing purpose and fully justify these decisions. Decisions can be revisited but changes could violate accountability and transparency and would require approval of the Executive Director or DPO, where appointed.

CORFAC must also ensure individuals whose data is being processed are informed of the lawful basis for processing their data and the intended purpose. This should occur via a privacy notice plus other available means (such as on-screen tool tips) where appropriate. This applies whether CORFAC collected the data directly from the individual or from another source.

When staff is making an assessment of the lawful basis and implementing the privacy notice for the processing activity, staff members must have this approved by the Executive Director or DPO, where appointed.

Special Categories of Personal Data

What are Special Categories of Personal Data?
Processing of 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 is prohibited with limited exceptions. If a potential need arises regarding potential processing of such special categories of data, consultation with the Executive Director or DPO, where appointed, and legal counsel should be made to determine if exceptions apply.

Responsibilities
CORFAC responsibilities include:
- Develop and implement a GDPR compliance policy
- Maintain custody of proper documentation for the personal data held by and processed for CORFAC
- Develop and enforce procedures in accordance with the GDPR to ensure protection of all the rights of data subjects
- Require staff identification of the lawful basis for processing data
- Ensure consent procedures are lawful
- Implement and review procedures to detect, report and investigate personal data breaches
- Store, process and transfer data in safe and secure ways
- Honor rights of data subjects under the GDPR
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Staff responsibilities include:
- Learn and completely understand the data protection obligations of CORFAC
- Check and assure that data processing activities you see, manage or handle comply with the CORFAC policy and are justified
- Avoid use of data in any unlawful way
- Avoid storing or enabling others to store data improperly

- Avoid being careless with personal data or otherwise cause a breach of data protection laws and CORFAC policies through your actions
- Comply with this policy
- Raise concerns, notify the Executive Director of any breaches or errors and report anything suspicious or contradictory to this policy or legal obligations without delay to the Executive Director or DPO, where appointed
- Assist with providing prompt response and compliance to data subject requests for access, portability, correction, deletion and other rights
- Assist with data protection impact assessments
- Update and maintain departmental GDPR documentation in CORFAC's GDPR database/spreadsheet.

Responsibilities of the Executive Director:

- Oversee design and implementation of controls built into CORFAC systems that automate and reinforce the principles of this policy such as data minimization, automatic expirations, security measures, pseudonymization, transparency in user interfaces, self-help interfaces for data subjects requesting their data
- Implement measures to reduce human error that can lead to violations of the principles
- Monitor staff compliance with record keeping in CORFAC's GDPR documentation database/spreadsheet
- Keep the Board of Directors updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies regularly
- Arrange data protection training and provide advice for all staff members and those included in this policy
- Answer questions on data protection from staff, board members and other stakeholders
- Respond to clients and employees who wish to know which data is being held on them by CORFAC
- Check and approve third parties that handle CORFAC's data including review of contracts or agreements regarding data processing

Responsibilities of the DPO (if appointed):

- Work independently and autonomously to ensure compliance without fear of reprisal
- Report to the CORFAC Executive Director
- Advise employees on obligations under the GDPR
- Complete compliance audits
- Work with supervisory authorities

Responsibilities of the IT and Web Managers:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Design and implement controls built into CORFAC systems and vendor systems that automate and reinforce the principles of this policy such as data minimization, automatic expirations, security measures, pseudonymization and transparency in user interfaces
- Create "privacy dashboards" for data subjects that (1) facilitate refreshing consent at appropriate intervals, (2) includes preference-management tools for privacy options, (3) makes it easy for individuals to withdraw their consent at any time and publicizes how to do so, (4) provides a method to request information on data possessed and (5) delete or transfer a person's data if permissible and required under the law
- Devise methods facilitating IT to act on disclosure requests regarding data subject's information and changing or withdrawing consents, plus rights to be forgotten, including plans for third-parties and disaster recovery backup files
- Make available to designated staff a departmental GDPR documentation database/spreadsheet for CORFAC
- Design, implement and offer systems that provide remote access to a secure self-service system which would provide individuals with direct access to their information to satisfy access and portability tests
- Check and scan security hardware and software regularly to ensure it is functioning properly
- Research and vet third-party services, such as cloud services CORFAC is considering to store or process data

Collective Responsibilities

Accuracy and Relevance

CORFAC will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. CORFAC will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this, would otherwise reasonably expect this or legally obligated to process. Individuals may ask that CORFAC correct inaccurate personal data relating to them. If staff believes that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Executive Director or DPO, where appointed.

Data Security

CORFAC staff must and will keep personal data secure against loss or misuse. Where other organizations process personal data as a service on behalf of CORFAC, the Executive Director or DPO, where appointed, will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organizations. Data should be encrypted.

Storing Data Securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorized personnel cannot access it
- Printed data will be shredded when no longer needed or discarded using an approved vendor
- CORFAC IT Policies must and will be followed
- All computers and data accessible by computer must and will be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks or other portable storage devices must and will be encrypted or password protected and locked away securely when they are not being used
- The Executive Director must approve any cloud based storage media used to store data
- Servers containing personal data must and will be kept in a secure location
- Data will be regularly backed up in line with CORFAC's backup procedures
- Data will never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must and will be approved and protected by security software
- Disaster recovery systems and plans are required and in place
- Testing, assessing and evaluating of system must and will be completed regularly
- All feasible technical and practical measures must and will be put in place to keep data secure

Data Retention

CORFAC must and will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case taking into account the reasons that the personal data was obtained but should be determined in a manner consistent with the CORFAC data retention policy and the law.

Transferring Data Internationally

There are restrictions on international transfers of personal data. CORFAC must and will not transfer personal data abroad or anywhere else outside of normal rules and procedures without express permission from the Executive Director or DPO, where appointed.

Rights of individuals

Individuals have rights to their data which the CORFAC staff must and will respect to the best of our ability in accordance with detailed requirements in the law. In broad terms, CORFAC must and will ensure individuals can exercise their rights in the following ways:

1. **Right to be informed.** The law requires transparency, meaning CORFAC must and will plainly disclose who it is and what personal data is being collected in no uncertain terms. CORFAC must and will also make disclosures to a data subject when information is received from others concerning the data subject. The disclosures must meet the detailed requirements of the law. With regard to all rights of the data subject as enumerated below, they have a right to responsiveness to their requests of CORFAC without "undue delay" and absolutely no longer than 30 days. In general, responses must be free of charge.

2. **Right of access.** Where requested by a subject, CORFAC must and will promptly disclose whether it is processing data on the subject, what the data is and the legal basis for the usage. The disclosure must and will set forth specific details enumerated in the GDPR.
3. **Right to rectification**. A data subject has the right to have inaccurate personal data promptly corrected and incomplete personal data completed.
4. **Right to erasure**. This is also known as the "right to be forgotten." A data subject has the right to ask CORFAC to erase and cease using their information. CORFAC is expected to use technological means to make this happen and make reasonable efforts to prevent others from processing the data where it was made public. The right is not absolute. Exceptions include justifiable reasons to keep the data, such as for a contractor pursuant to a litigation hold, etc.
5. **Right to restrict processing**. In some situations, complete erasure goes too far or does not adequately meet interests of a data subject. For instance, limitations can be appropriate during accuracy checks, litigation holds and objections to scope of use of the data under GDPR. As middle ground, a data subject has a right to have restrictions put on the processing of data either permanently or for time needed for legal and practical reasons.
6. **Right to data portability**. CORFAC must and will provide a method for a data subject to easily electronically download or transfer their data to another controller. The data must be in a readily readable format that can be fed into other systems, including online systems. A CSV file could be compliant. However, an encrypted, uncopiable pdf version would not likely suffice.
7. **Right to object**. In many instances, CORFAC's lawful basis for processing data will be based on "legitimate interest." CORFAC must and will forthrightly alert a data subject of their right to object to processing on that basis. Upon receiving an objection, CORFAC must and will cease processing until it provides compelling legitimate grounds for processing the data. Next, where CORFAC is processing data for direct marketing or profiling, CORFAC must and will cease processing upon receiving an objection from the data subject. Again, CORFAC must and will provide notice of the right to object at the outset.
8. **Rights in relation to automated decision making and profiling.** CORFAC must and will notify data subjects where automated systems (e.g. AI) evaluate or make judgments about them and about their right to object to such profiling and rights to request human intervention. Automated processing requires increased internal scrutiny and written justification including an official Data Processing Impact Assessment. Examples include an employment screening aptitude test or characteristic profiling.

Privacy Notices

A privacy notice is a statement CORFAC shares with others to describe how CORFAC collects, uses, retains and discloses personal data. CORFAC must and will provide the notice at the time of collection of the data. If CORFAC obtains data from a third-party, privacy notices must be provided within a reasonable time. Privacy notices are not just for website or app usage. Notice requirements also apply to paper forms and phone services for example. CORFAC will have many privacy notices wherein each is customized to the needs of the user and based on the information within CORFAC's GDPR documentation database/spreadsheet.

CORFAC Privacy Policy

What information we collect

We collect information from you when you place an order or respond to a survey or poll. When ordering or registering on our site, as appropriate, you may be asked your name, email address, mailing address, phone number or credit card information. You may, however, visit our site anonymously.

What do we use your information for?

Any of the information we collect from you may be used in one of the following ways: To process a transaction: Your information, whether public or private, will not be sold, exchanged, transferred or given to any other company for any reason whatsoever, without your consent, other than for expressed purpose of delivering the purchased product. To send a periodic email: The email address you provide for order processing will only be used to send you information and updates pertaining to your order.

How do we protect your information?

We implement a variety of security measures to maintain the safety of your personal information when you place an order or enter, submit or access your personal information. We offer the use of a secure server. All supplied sensitive/credit card information is transferred via Secure Socket Layer technology and then encrypted to out payment gateway provider's database, which is only accessible by those authorized with special access rights to such systems and who are required to keep the information confidential. After the transaction, your private information will not be kept on file for more than 60 days.

Do we use cookies?

We do not use cookies.

Do we disclose any information to outside parties?

We do not sell, trade or otherwise transfer to outside parties identifiable information. This does not include trusted third parties who assist us in operating our website, conducting our business or servicing you, so long as those parties agree to keep this information confidential. We may release your information when we believe release is appropriate to comply with law, enforce our policies or protect ours and others' rights, property or safety. However, non-personal identifiable visitor information may be provided to other parties for marketing, advertising or other uses.

Children's Online Privacy Policy Protection Act Compliance

We are in compliance with COPPA. We do not collect any information from anyone 13 years of age or younger. Our website, products and services are directed to people who are at least 13 years old or older.

Your consent

By using our website, you consent to our website's privacy policy.

What's not Acceptable

One-size-fits-all, boilerplate, lengthy, take-it-or-leave-it type notices are unacceptable. Likewise, notices that are vague, fail to explain what happens to information, fails to explain with whom information is shared and fails to advise users about how to access their information are unacceptable.

Key Concepts

A major goal of GDPR is transparency. User's rights must and will be spelled out in a concise, transparent, intelligible and easily accessible form, using clear and plain language. To facilitate this, the law promotes using standardized icons in order to give an easily visible, intelligible and meaningful overview of the intended processing. Where the icons are presented electronically they must be machine-readable.

Good Practices

Good design practices include:

- Specificity: notice targeted to each piece of data
- Layering: provide key notice points immediately in a clean easy-to-read format with a link to the detailed information
- Just in time notices: provide notices in tool tips for text input fields
- Icons and symbols: provide just in time information using a pop up from an icon (e.g. question mark icon or small "i" icon); use themed icons to represent concepts.

The 15 Components of Privacy Notices

The following information must and will be included in the comprehensive CORFAC privacy notices:

1. Name and contact information for the CORFAC Executive Director and DPO, where appointed
2. Data being collected
3. All purposes for which the data will be used
4. "Lawful basis" for collecting each piece of data
5. Where a lawful basis is "legitimate interests," an explanation of those legitimate interests
6. Recipients or categories of recipients of the data
7. Plans to share the data abroad
8. Retention period or criteria defining the retention period for which data will be stored
9. Rights of the data subject to access, rectification, erasure, restriction, objection and data portability along with methods to exercise those rights
10. If consent was the lawful basis for data collection, the right to withdraw consent without repercussions
11. Rights to complain to a Supervisory Authority and methods to exercise those rights
12. If the "lawful basis" is a contractual or legal obligation (e.g. statutory), possible consequences for any failure to provide the data
13. Existence of automated decision making, including profiling and information about how those decisions are made, their significance and consequences to the data subject

For personal data provided to CORFAC by others, the privacy notice must and will also include:

14. Category of the personal data
15. Source of the personal data and whether it came from publicly available sources

The law provides exceptions where the data subject already has the information above or disproportionate effort would be required to deliver the notice.

Subject Requests

Self-Service Systems

Where possible and economically feasible, CORFAC will design, implement and offer systems that provide remote access to a secure self-service system in real time which would provide individuals with free direct access to the information to satisfy access, erasure, correction, objection and portability requests. CORFAC will use reasonable measures to verify the identity of a data subject who requests access in particular in the context of online services and online identifiers. CORFAC will not retain personal data for the sole purpose of being able to react to potential requests.

Request Accommodation Without Self-Service Systems

Requests by data subjects to enforce their rights under GDPR need not come in any special form. Responses must be in writing unless the subject requests otherwise. CORFAC staff must and will make best efforts to respond to requests from data subjects regarding any of their data being used by CORFAC. The first step is to use reasonable means to verify the identity of the requestor.

Once the identity has been reasonably identified, CORFAC staff must and will promptly disclose whether it is processing the data or has access to it. Where CORFAC is storing or processing data, CORFAC must and will provide an individual with a copy of the information free of charge. This must occur without delay and within one month of receipt. CORFAC will provide access to information in a commonly used electronic format unless requested otherwise.

If complying with the request is complex or numerous, the deadline can be extended by two months but the individual must be informed within one month. You must obtain approval from the Executive Director or DPO if elected, before extending the deadline.

CORFAC can refuse to respond to certain requests and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, CORFAC can request the individual specify the information they are requesting.

Once a subject access request has been made, CORFAC staff must and will not change or amend any of the data that has been requested. Doing so could be a civil or criminal offense.

Subject Access Requests
A subject has the right to request that CORFAC promptly disclose whether it is processing data on the subject, what the data is and the legal basis for the usage. The disclosure must set forth specific details enumerated in the GDPR. The subject also has the right to take the data and reuse it. The data must be in a readily readable format that can be fed into other systems including online systems. A CSV file could be compliant. However, an encrypted, uncopiable pdf version would not likely suffice. Preferably requests will be handled by self-service electronic means. Otherwise CORFAC staff must and will respond in accordance with this policy.

Data Portability Requests
CORFAC must and will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. CORFAC must and will provide this data either to the individual who has requested it or to the data controller they have requested it be sent to. This must and will be done free of charge and without delay and no later than one month. This can be extended to two months for complex or numerous requests but the individual must and will be informed of the extension within one month and you must receive express permission from the Executive Director or DPO, if appointed, first. Preferably requests will be handled by self-service electronic means. Otherwise staff must and will respond in accordance with this policy.

Erase and Restriction Requests
Subject to important exceptions, individuals have a right to have their data erased and for processing to cease or for restrictions to be placed on processing. Exceptions include justifiable reasons to keep the data such as for a contract or pursuant to a litigation hold, etc. Preferably requests will be handled by self-service electronic means. Otherwise CORFAC staff must and will respond in accordance with this policy. Where restrictions are lifted, the data subject must be notified.

If data has been made public and fell into the hands of other controllers, CORFAC must and will, taking into account available technology and the cost of implementation, take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. Also, if CORFAC disclosed data to others and the subject's requests erasure or restrictions, those requests must be forwarded to everyone whom the data was shared, unless it is impossible to do so.

Objections
Individuals have the right to object to their data being used processing based on legitimate interests, profiling, direct marketing and research and statistics. CORFAC must and will cease processing unless the organization can either show a compelling legitimate interest or legal reasons. If possible, requests will be handled by self-service electronic means. Otherwise, CORFAC staff must and will respond in accordance with this policy.

Third-Party Controllers and Processors
As a data controller and data processor, CORFAC must and will have written contracts in place with any third-party data controllers or data processors CORFAC engages. The contract must contain specific clauses which set out liabilities, obligations and responsibilities under the GDPR including agreements to:

a) Process the personal data only on documented instructions from the controller
b) Only authorize persons to process the personal data who have committed themselves to confidentiality
c) Take all measures required pursuant to GDPR Article 32 on security

d) Obtain CORFAC's permission to engage subcontractors for the work and ensure the same obligations apply to subcontractors
e) Make best efforts to help CORFAC respond to data subject's rights
f) Assist in compliance obligations pursuant to GDPR Articles 32 to 36
g) Delete or return all the personal data to the controller after the end of the provision of services relating to processing and delete existing copies unless law requires storage of the personal data
h) Make available to the controller all information necessary to demonstrate compliance with the obligations of GDPR Article 32.

Criminal record checks
CORFAC may and will only carry out criminal records checks where permissible by law. Processing of personal data relating to criminal convictions and offenses must provide for appropriate safeguards for the rights and freedoms of data subjects.

Audits, monitoring and training

Data Audits
Regular data audits will be conducted to manage and mitigate risks

Monitoring
All CORFAC staff must and will observe this policy. The Executive Director has overall responsibility for this policy. CORFAC will keep this policy under review and amend or change as required. CORFAC staff must and will notify the Executive Director and DPO, where appointed, of any breaches of this policy.

Training
CORFAC staff will receive adequate training on provisions of data protection law specific for each person's role. CORFAC staff must and will complete all training as requested. If CORFAC staff changes roles or responsibilities, responsibility lies with that person to requesting new data protection training relevant to the new role or responsibilities. If staff requires additional training on data protection matters, contact the Executive Director.

Reporting breaches
A "personal data breach" is a breach of CORFAC's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
.
Notice to Individuals
If a breach is likely to result in a high risk to the rights and freedoms of natural persons, CORFAC must and will give notice to that person without undue delay. The notice must be in clear and plain language and include (1) the nature of the breach, (2) CORFAC contact information, (3) likely consequences of the breach and (4) measures planned or taken to mitigate damage.

Exceptions to the reporting requirement arise in three scenarios: (1) the data taken is encrypted, (2) CORFAC measures reduce the high risk to people's rights or (3) individual notice would require disproportionate effort wherein a public notice serves the purpose effectively.

Notice to Supervisory Authority
Where CORFAC can identify a Supervisory Authority under GDPR, CORFAC will without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

As a U.S.-based organization without any establishment in the EU and limited activity, the GDPR, as of May 2018, fails to identify desired reporting procedures for such an organization.

With regard to a potential Lead Supervisory Authority, Controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative.

The cyber insurer will be consulted immediately to assist with determining the best and proper approach to sending notices under the law.

Failure to Comply

CORFAC International takes compliance with this policy very seriously. Failure to comply puts both staff and the organization at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under CORFAC procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Executive Director.