Privacy Policy

Nuzl SVG LLC

Registered address: Beachmont Business Centre, Suite 379, Kingstown, Saint Vincent and the Grenadines

Contact address: Beachmont Business Centre, Suite 379, Kingstown, Saint Vincent and the Grenadines

Policy prepared by:	Data Protection Officer
Approved by board/management on:	19.05.2022
Policy became operational on:	19.05.2022
Next review date:	19.05.2023

Content

Introduction

This Privacy Policy sets out the policy which Nuzl SVG LLC group (hereinafter NUZL) has adopted in order to facilitate compliance with the General Data Protection Regulations (the "GDPR") together with local data protection (hereinafter - "DPR") regulations worldwide when we establish and manage customer and business relationships and execute transactions, etc.

The GDPR together with local data protection regulations regulate the processing of personal data.

Personal data is defined as 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.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the DPR. This can include:

- names of individuals;
- an identification number;
- location data;
- an online identifier;
- email addresses;
- telephone numbers;
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and
- any other information relating to individuals

Processing covers 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Data Protection are underpinned by six important principles. These say that personal data must:

1. Be processed fairly and lawfully ('lawfulness, fairness and transparency')
2. Be obtained only for specific, lawful purposes ('purpose limitation')
3. Be adequate, relevant and not excessive ('data minimisation')
4. Be accurate and kept up to date ('accuracy')
5. Not be held for any longer than necessary ('storage limitation')
6. Be protected in appropriate ways ('integrity and confidentiality')

Nuzl as a controller of personal data is responsible for compliance with the principles set above.

Abbreviations

'CTO' means Chief Technology Officer;

'DPI' means Data Protection Inspectorate;

'DPO' means Data Protection Officer;

'EEA' means European Economic Area;

'EU' means European Union;

'WW' means worldwide.

'SVG' means Saint Vincent and Grenadines

Terms and Definitions

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

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

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

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

'Supervisory authority' means an independent public authority which is established to be responsible for monitoring the application of the DPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the client's territory or residentship;

'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

1. Scope

This policy applies to:

- the offices of Nuzl;
- all staff and volunteers of Nuzl; and

- all contractors, suppliers and other people (authorised persons) working on behalf of the Nuzl.

A copy of this Policy will be supplied to each such person mentioned above. The requirements set out in this Policy are mandatory unless otherwise stated and must be followed by all persons involved in the data processing activities. It is the responsibility of each such person to acquaint themselves with the requirements of this Policy. Failure to comply with this Policy may constitute a serious disciplinary offence and could result in dismissal.

2. Purpose

Nuzl processes personal data in various situations and in relation to various categories of individual. This Policy deals with personal data collected in the context of the establishment and management of our customer relationships and the execution of transactions on the instructions of our customers and as well as with personal data of individuals who are employees, contractors and partners of Nuzl. The individuals to whom personal data relate, whether customers or otherwise, are known as "data subjects".

3. Policy Statement

Our principal obligations under the DPR include:

- respect individuals' rights;
- processing personal data lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collecting personal data for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes ('purpose limitation');
- ensuring that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- ensuring that personal data are accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- ensuring that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');
- ensuring that personal data are 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, using appropriate technical or organisational measures ('integrity and confidentiality').
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently; and
- responding appropriately when data subjects seek to exercise their statutory rights of access, correction and objection.

This Policy is supplementary to our other published policies.

4. Data protection risks

This policy helps to protect Nuzl from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.

- Failing to offer choice. For instance, all individuals should be free to choose how the company uses personal data relating to them.
- Failing to comply with the DPR principles. For instance, collect or transfer personal data without data subject's consent.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to personal data.
- Financial damage. For instance, fines imposed by the supervisory authority.

5. General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees/authorised persons can request it from their line managers.
- Nuzl will provide training to all employees to help them understand their responsibilities when handling data.
- Persons, whom this policy apply to, should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Data should not be disclosed to unauthorised people, either within the company or externally.
- Persons, whom this policy apply to, should sign the Declaration of acceptance of Personal Data Protection requirements set by this Privacy Policy.

6. Responsibilities

Everyone who works for or with Nuzl has some responsibility for ensuring data is collected, stored and handled appropriately.

Each department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

The Board of Directors is ultimately responsible for ensuring that Nuzl meets its legal obligations.

The Data Protection Officer is responsible for:

- Monitoring compliance with the DPR and other data protection provisions.
- Keeping the Board updated about data protection responsibilities, risks and issues.
- Monitoring compliance with the policies of the controller or processor in relation to the protection of personal data.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Providing advice where requested as regards the data protection impact assessment and monitor its performance.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data Nuzl holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Keeping controller's and processor's processing activities records up to date.
- Cooperating with the supervisory authority and act as the contact point on issues relating to processing and to consult, where appropriate, with regard to any other matter.

If you have any questions about this Policy or application in particular circumstances, you should consult the Data Protection Officer.

The Marketing Team is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

7. Personal data processing for different categories of data subjects

7.1. Data processing for the employment relationship and company's business activity

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other Nuzl group companies.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorisation to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

7.1.2. Lawful basis for personal data processing

7.1.2.1. Data processing pursuant to legal authorisation

The processing of personal employee data is also permitted if national legislation requests, requires or authorises this. The type and extent of data processing must be necessary for the legally authorised data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

7.1.2.2. Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorised through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives. The agreements must cover the specific purpose of the

intended data processing activity, and must be drawn up within the parameters of national data protection legislation.

7.1.2.3. Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed about the identity of Nuzl as a data controller, the purposes of data processing and any third parties or categories of third parties to whom the data might be transmitted.

7.1.2.4. Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of the Nuzl. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

7.1.3. Personal data processed by Nuzl

Nuzl processes the following personal data:

Board of Directors records: These may include:

- name, address and contact details of each member of the Board of Directors and secretary;
- records in relation to appointments to the Board;
- Minutes of Board of Directors meetings and correspondence to the Board which may include references to particular individuals.

Format: manual record (personal file within filing system) and/or computer record (database).

Purpose: keeping a record of Board appointments, documenting decisions made by the Board.

Staff records (including volunteers, contractors): These may include:

- name, address and contact details, personal identification code;
- original records of application and appointment;
- record of appointments to promotion posts;
- details of approved absences (career breaks, parental leave, study leave etc.);

- details of work record (CV, qualifications, classes taught, subjects etc.);
- details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress;
- health data of employees;
- e-mail messages.

Note: a record of grievances may be maintained which is distinct from and separate to individual personnel files.

Format: manual record (personal file within filing system) and/or computer record (database).

Purpose: to facilitate the payment of staff, to facilitate pension payments in the future, a record of promotions made.

7.1.4. Special categories of personal data (sensitive personal data) and processing of personal data relating to criminal convictions and offences

Sensitive personal data is defined as personal data consisting of information as to:

a) physical or mental health or condition;

b) racial or ethnic origin;

c) political opinion;

d) religious or philosophical beliefs;

e) trade union membership;

f) genetic data, and biometric data where processed to uniquely identify an individual;

g) sex life or sexual orientation.

Sensitive personal data can be processed only under certain conditions. Nuzl does not seek to collect or process personal data identified from b) to g) in the list above. Nuzl's employees should not collect or process sensitive personal data for specified purposes and should delete them if they become aware that we have collected them, except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPR.

Data that relates to a crime can be processed only under special requirements under national law.

7.1.5. Automated decisions

Where personal data is processed automatically as a part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing should not be the sole basis for the final decision taking.

If at any time Nuzl will use such approach of automated decision, this automated processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee or contractor. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject will also be informed of the facts and results of automated individual decisions and the possibility to respond.

7.1.6. Telecommunications and internet for employees

Telephone equipment, email addresses and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorised

use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or internet use. To defend against attacks on the IT infrastructure or individual users, protective measures will be implemented for the connections to the Nuzl 's network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person will be made only in a concrete, justified case of suspected violations of laws or policies of the Nuzl. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the company's policies.

7.2. Data processing for the business relationship (third party vendors, suppliers and partners)

Personal data of the relevant third party vendors, suppliers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfil other requests of the prospect that relate to contract conclusion. Third party vendors, suppliers and partners can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the third party vendors, suppliers and partners must be complied with.

7.2.1. Lawful basis for personal data processing

7.2.1.1. Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

7.2.1.2. Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed about the identity of Nuzl as a data controller, the purposes of data processing and any third parties or categories of third parties to whom the data might be transmitted. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

7.2.1.3. Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of the Nuzl. Legitimate interests are generally of a legal or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

7.2.2. Personal data processed by Nuzl

Nuzl processes the following personal data:

Third party vendors', suppliers' and partners' records: These may include:

- name, address and contact details of third party vendors, suppliers and partners who are natural persons;
- name, position, address and contact details of employees or contact persons of the third party vendors, suppliers and partners who are legal persons;

- records of appointments or documents of authorisation of signature;
- communication between Nuzl and party third vendors, suppliers and partners;
- due diligence records on third party vendors, suppliers and partners, where applicable.

Format: manual record (personal file within filing system) and/or computer record (database).

Purpose: establish, execute and terminate a contract.

7.2.3. Special categories of personal data (sensitive personal data)

Nuzl does not seek to collect or process personal data identified by the GDPR as "sensitive" for business relationship purposes. Nuzl's employees should not collect or process sensitive personal data for specified purposes and should delete them if they become aware that we have collected them, except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPR. Sensitive personal data is defined as personal data consisting of information as to:

- physical or mental health or condition;
- racial or ethnic origin;
- political opinion;
- religious or philosophical beliefs;
- trade union membership;
- genetic data, and biometric data where processed to uniquely identify an individual;
- sex life or sexual orientation.

If at any time Nuzl will need to process such sensitive personal data in the future due to the changes in the purposes of data processing, the processing will be carried out in accordance with the principles set out in the GDPR.

7.2.4. Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

It means to process personal data about criminal convictions or offences, Nuzl must have both a lawful basis and either legal authority or official authority for the processing.

Currently, Nuzl does not seek to collect or process personal data relating to criminal convictions and offences.

If at any time Nuzl will need to process such personal data in the future due to the changes in the purposes of data processing, the processing will be carried out in accordance with the principles set out in the GDPR.

7.2.5. Automated decisions

Where personal data is processed automatically as part of the business relationship, and specific personal details are evaluated, this automatic processing is not the sole basis for the final decision taking.

If at any time Nuzl will use such approach of automated decision taking, this automated processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee or partner. To avoid erroneous decisions, a test and plausibility check must be made by an employee of Nuzl.

7.3. Data processing for the customer relationship

7.3.1. Data processing for a customer contractual relationship (service providing)

Personal data of the relevant customers (users) can be processed in order to establish, execute, terminate a contract in the form of Nuzl's Terms and Conditions published at website http://hexn.io and for the purposes of providing the customers with the company's products and services. Customers can be contacted during the on-boarding process using the information that they have provided and requested to provide additional information, including personal data, required by relevant legislation.

We may collect, use, store, share and disclose different kinds of Personal data about you which (**for purely indicative purposes**) we have grouped together as follows. For avoidance of doubt, categories marked in blue are not applicable to non-customers (i.e. individuals who do not hold a registered customer account with us).

- **Identity Data** includes your first name, maiden name (where applicable), last name, username or similar identifier, marital status, title, nationality, date of birth, gender, identity card and/or passport number.
- **Contact Data** includes address, billing address, email address and contact number (telephone and/or mobile).
- **AML and KYC Data** includes the following due diligence documentation and information on you:

  (i) copy of your national identity document, passport and/or driver's licence, (ii) proof of residence (for example, a recently issued utility bill), (iii) a 'selfie' (for identity verification), (iv) KYC database checks, (v) fraud database checks and (vi) any documentation or information which we may be from time to time:

1. required to collect to ensure compliance with any applicable legislation (including applicable foreign laws) and global AML/KYC practices; and/or
2. otherwise mandated to collect by any competent authority, including, as applicable, any other documentation or information which may be mandated on us from time to time by applicable law and by any other competent authority or related legislation (including overseas authorities and applicable foreign laws).

- **Enhanced KYC Data** applies in respect of payments which exceed a set threshold and includes, at a minimum, the following enhanced customer due diligence documentation and information: source of funds and source of wealth.
- **Financial Data** includes your wallet and private key details.
- **Transaction Data** includes details about:

1. your subscriptions, purchases and transactional activity;
2. your transactional history on the Platform;
3. your use of the Services (including your service requests);

4. the payments made to and from you.

- **Portfolio Data** includes details about the tokens credited to your account.
- **Usage Data** includes details about how you use our Platform and the Websites.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices which you (whether a client or otherwise) use to access and browse the Websites.
- **Website Visit Data** includes the full Uniform Resource Locators (URL), clickstream to, through and from the Website (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us or our third parties and your communication preferences. This may include information whether you have subscribed or unsubscribed from any of our mailing lists, attended any of our events, or accepted any of our invitations.

We will also collect, use and process any other information that you voluntarily choose to provide or disclose to us where relevant for processing your token requests and/or providing you with your requested Services. Any such information that we receive from you would fall under the '**Transaction Data**' category.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your Personal data but is not considered Personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Website Visit Data to calculate the percentage of users accessing a specific feature of the Website. However, if we combine or connect Aggregated Data with your Personal data so that it can directly or indirectly identify you, we treat the combined data as Personal data which will be used in accordance with this Policy.

7.3.2. Data processing for advertising purposes

If the data subject contacts Nuzl to request information (e.g. request to receive information material about a product/service), data processing to meet this request is permitted.

Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone.

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

7.3.3. Lawful basis for personal data processing

7.3.3.1. Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

7.3.3.2. Consent to data processing

Data can be processed following consent by the data subject when the data processing is performed for the advertising purposes. Before giving consent, the data subject must be informed about the identity of Nuzl as a data controller, the purposes of data processing and any third parties or categories of third parties to whom the data might be transmitted. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

7.3.3.3. Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of the Nuzl. Legitimate interests are generally of a legal or commercial nature (e.g. avoiding breaches of Terms and Conditions or any relevant AML/CFT legislation). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

7.3.4. Personal data processed by Nuzl

Nuzl processes the following personal data:

Customers' (users') records: These may include:

- customer's name, address and contact details;
- financial and transaction information;
- communication between Nuzl and customer;
- due diligence records:
    - results of electronic verification of customer's identity or identity document;
    - results of check against different sanction lists;
    - results of check against the PEP lists;
    - identification documents (passport, ID card, driver licence, etc.)
    - address confirmation documents;
    - information on and confirmation documents of the source of funds and source of wealth;
    - legal documents for corporate customers where the information about the individuals may be present (Memorandum and Articles of Association, Resolution of an Appointment of Director, Shareholder register, Declaration of UBO, etc.);
- cookie files;
- geolocation data;

- log files (Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, platform type, date/time stamp, and number of clicks);
- adverse media data, etc.

Format: manual record (personal file within filing system) and/or computer record (database).

Purpose: establish, execute and terminate a customer relationship in accordance with the company's Terms and Conditions; services providing; compliance with the relevant AML/CTF legislation; evaluate, monitor and analyse the use of the website https://hexn.io and its traffic patterns to help improve the Website and services; provide customers with personalised content based on his/her use of the Website; enable customers to more easily use the Website by remembering and using contact information, purchasing information, and registration information; minimize risks and identify or investigate fraud and other illegal activities.

7.3.5. Special categories of personal data (sensitive personal data)

Nuzl does not seek to collect or process personal data identified by the DPR as "sensitive" for customer relationship purposes. Nuzl's employees should not collect or process sensitive personal data for specified purposes and should delete them if they become aware that we have collected them, except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPR. Sensitive personal data is defined as personal data consisting of information as to:

- physical or mental health or condition;
- racial or ethnic origin;
- political opinion;
- religious or philosophical beliefs;
- trade union membership;
- genetic data, and biometric data where processed to uniquely identify an individual;
- sex life or sexual orientation.

If at any time Nuzl will need to process such sensitive personal data in the future due to the changes in the purposes of data processing, the processing will be carried out in accordance with the principles set out in the DPR.

7.3.6. Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

It means to process personal data about criminal convictions or offences, Nuzl must have both a lawful basis and either legal authority or official authority for the processing.

Currently, Nuzl does not seek to collect or process personal data relating to criminal convictions and offences.

If at any time Nuzl will need to process such personal data in the future due to the changes in the purposes of data processing, the processing will be carried out in accordance with the principles set out in the GDPR.

Note: Nuzl may collect and store personal data relating the offences as part of the customer's profile during the adverse media check if such data is publicly available. This information can help Nuzl to minimise risk that may arise as a result of entering into the customer relationship.

7.3.7. Automated decisions

Where personal data is processed automatically as part of the customer relationship, and specific personal details are evaluated, this automatic processing is not the sole basis for the final decision taking.

If at any time Nuzl will use such approach of automated decision taking, this automated processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee or partner. To avoid erroneous decisions, a test and plausibility check must be made by an employee of Nuzl.

7.3.8. User data and internet

When personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a Privacy Policy. Website Privacy Policy can be found by following the link http://hexn.io The privacy statement and cookie information is integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

When websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

8. Children's personal data

Our policy is not to knowingly provide services to or collect personal data and information from persons under 18 years of age. Our website is not directed or intended for children under this age. There should be a following caution on our website: 'If you are under 18 years of age, you should not provide personal data or information on our website. If you are the parent or guardian of a person under the age of 18 who you believe has disclosed personal data or information to us, please immediately contact us at dpo@hexn.io so that we may delete and remove such person's data from our system.'

9. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

9.1. Right to be informed

The data subject has right to be informed regarding the information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.

The information Nuzl supplies about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information Nuzl should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and the data protection officer	**V**	**V**
Purpose of the processing and the lawful basis for the processing	**V**	**V**

The legitimate interests of the controller or third party, where applicable	**V**	**V**
Categories of personal data		**V**
Any recipient or categories of recipients of the personal data	**V**	**V**
Details of transfers to third country and safeguards	**V**	**V**
Retention period or criteria used to determine the retention period	**V**	**V**
The existence of each of data subject's rights	**V**	**V**
The right to withdraw consent at any time, where relevant	**V**	**V**
The right to lodge a complaint with a supervisory authority	**V**	**V**
The source the personal data originates from and whether it came from publicly accessible sources		**V**
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	**V**	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	**V**	**V**
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month); If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

9.2. Right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information as shown in the table in section 7.1. Right to be informed.

Email subject access requests from individuals should be addressed to dpo@hexn.io. If the request is made electronically, the information should be provided in a commonly used electronic format. Postal requests should be sent to:

Data Protection Officer

Beachmont Business Centre, Suite 379,

Kingstown, Saint Vincent and the Grenadines

DPO or the relevant person must verify the identity of the person making the request.

Nuzl will provide a copy of the information free of charge. However, Nuzl can charge a 'reasonable fee' or refuse to respond when a request is manifestly unfounded or excessive, particularly if it is repetitive. In such a case Nuzl shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Nuzl may also charge a reasonable fee to comply with requests for further copies of the same information. The fee is based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt of the request.

Nuzl will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, Nuzl will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Access to Personal Data request form is attached in the 'Annex I' to this Privacy Policy.

9.3. Right to rectification

Individuals have the right to have personal data rectified if it is inaccurate or incomplete. If Nuzl has disclosed the personal data in question to others, it must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, Nuzl must also inform the individuals about these recipients.

To perform an action on request Nuzl should verify the identity of the natural person making this request. The additional information necessary to confirm the identity of the data subject should be requested.

Nuzl must respond to such request within 1 month. This can be extended by two months where the request for rectification is complex. Where Nuzl is not taking action in response to a request for rectification, it must explain why to the individual without delay and at the latest within one month of receipt of the request, informing him or her of his or her right to complain to the supervisory authority and to a judicial remedy.

9.4. Right to erasure ('right to be forgotten')

This right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the DPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

To perform an action on request Nuzl should verify the identity of the natural person making this request. The additional information necessary to confirm the identity of the data subject should be requested.

If Nuzl has disclosed the personal data in question to others, it must contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, Nuzl must also inform the individuals about these recipients.

Information on action to the individual must be provided without delay and at the latest within one month of receipt of the request.

Nuzl will be able to extend the period of compliance by a further two months where necessary. If this is the case, Nuzl will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where Nuzl is not taking action in response to a request for erasure, it must explain why to the individual without delay and at the latest within one month of receipt of the request, informing him or her of his or her right to complain to the supervisory authority and to a judicial remedy.

9.5. Right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data.

Nuzl will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, Nuzl should restrict the processing until it has verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and Nuzl is considering whether its organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If Nuzl no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

To perform an action on request Nuzl should verify the identity of the natural person making this request. The additional information necessary to confirm the identity of the data subject should be requested.

Information on action to the individual must be provided without delay and at the latest within one month of receipt of the request.

Nuzl will be able to extend the period of compliance by a further two months where necessary. If this is the case, Nuzl will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If Nuzl has disclosed the personal data in question to others, it must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, Nuzl must also inform the individuals about these recipients.

Where Nuzl is not taking action in response to a request for restrict processing, it must explain why to the individual without delay and at the latest within one month of receipt of the request, informing him or her of his or her right to complain to the supervisory authority and to a judicial remedy.

Nuzl must inform individuals when it decides to lift a restriction on processing.

9.6. Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

To perform an action on request Nuzl should verify the identity of the natural person making this request. The additional information necessary to confirm the identity of the data subject should be requested.

Nuzl must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge. If the individual requests it, Nuzl may be required to transmit the data directly to another organisation if this is technically feasible. However, Nuzl is not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, Nuzl must consider whether providing the information would prejudice the rights of any other individual.

Nuzl must respond without undue delay, and within one month. This can be extended by two months where the request is complex or Nuzl receives a number of requests. Nuzl must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where Nuzl is not taking action in response to a request, it must explain why to the individual without delay and at the latest within one month of receipt of the request, informing him or her of his or her right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

9.7. Right to object

In general, individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Nuzl must stop processing the personal data unless:

- Nuzl can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

To perform an action on request Nuzl should verify the identity of the natural person making this request. The additional information necessary to confirm the identity of the data subject should be requested.

Nuzl must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse. Nuzl must deal with an objection to processing for direct marketing at any time and free of charge.

Nuzl must inform individuals of their right to object “at the point of first communication” and in Nuzl 's Privacy Policy. This must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

Information on action to the individual must be provided without delay and at the latest within one month of receipt of the request.

Nuzl will be able to extend the period of compliance by a further two months where necessary. If this is the case, Nuzl will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where Nuzl is not taking action in response to a request for object, it must explain why to the individual without delay and at the latest within one month of receipt of the request, informing him or her of his or her right to complain to the supervisory authority and to a judicial remedy.

9.8. Rights related to automated decision making including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Automated individual decision-making is a decision made by automated means without any human involvement.

The GDPR restricts companies from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone’s legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

Currently Nuzl does not use automated decision-making. If at any time it will become use automated decision-making, Nuzl must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
    - obtain human intervention;
    - express their point of view; and
    - obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that it can correct inaccuracies and minimise the risk of errors;

- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

10. Transfer to third parties

We will share personal data information with third party service providers, who are acting on behalf of Nuzl as our data processor.

Nuzl uses trusted third parties, who assist us in operating our website, conducting our business, or servicing our customers, so long as those parties agree to keep this information confidential. We may also disclose information when we believe disclosure is appropriate to comply with the law, enforce our policies, or protect ours or others' rights, property, or safety.

Where external companies are used to process personal data on behalf of Nuzl, responsibility for the security and appropriate use of that data remains with Nuzl.

11. International transfer of personal data

In some cases, Nuzl might transfer personal data to countries outside Saint Vincent and the Grenadines ('third country') for the purposes set out in this policy. Nuzl is committed to adequately protecting personal data information regardless of where the data resides and to providing appropriate protection for information where such data is transferred outside of the Saint Vincent and the Grenadines.

The legal basis for the transfer of personal data to third country is Nuzl's or the subcontractors' Binding Corporate Rules, European Commission's Standard Contractual Clauses for the transfer of personal data to processors established in third countries ('Standard Contractual Clauses'), the EU-U.S. Privacy Shield Framework, alternative data export mechanisms for the lawful transfer of personal data (as recognised under EU data protection laws) or other legal basis.

If there is no legally based right to transfer the data to a third country, the basis of the transfer is the data subject's explicit consent to the transfer which is asked separately, in which case the data subject is hereby informed of the risks of such transfer. Such risks may include that the level of protection of individuals arising out of the EU laws is not necessarily guaranteed in those third countries, which can include e.g. that third parties or authorities can have access to the data to the wider extent than according to EU laws, the security methods might not be at the level as regulated under EU laws and the individuals might not have effective remedies to inspect their data, rights to access their data or get their data corrected at the level as regulated under EU laws.

Also, the individual might use Nuzl products or services in third countries or the individual might contact Nuzl from locations in third countries. In such case, it is deemed that the individual has consented to the transfer of the relevant personal data to third country.

In the absence of basis specified above a transfer or a set of transfer of personal data by Nuzl to a third country shall take place only on one of the following conditions:

- the transfer is necessary for the performance of the contract between the data subject and data controller or the implementation of pre-contractual measures taken at the data subject's request

  Note: data transfers on the grounds of this derogation may take place where the transfer is occasional and necessary in relation to a contract;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

  Note: data transfers on the grounds of this derogation may take place where the transfer is occasional and necessary in relation to a contract;

- the transfer is necessary for important reasons of public interest;

- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary to protect the vital interests of the data subject.

More details on derogation for specific situations in regards of a personal data transfer can be found in the Guidelines on Article 49 of Regulation 2016/679 published by the Article 29 Data Protection Working Party.

12. Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Nuzl will disclose requested data. However, as a data controller the organisation will ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary.

13. Personal data breaches

13.1. General information

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Types of personal data breaches:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Personal data breaches examples:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

13.2. The possible consequences of a personal data breach

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal

data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible.

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) of the GDPR or on its own.

13.3. Notification of data breach to supervisory authority and communication to data subject

More detailed information in regards of breach notification to supervisory authority and breach communication to data subject are covered by the separate internal policy 'Personal Data Breach Notification and Communication Procedures'.

13.4. Internal report of a personal data breach to DPO

If any person, whom this policy applies to, become aware of personal data breach, he or she shall without undue delay notify the DPO and provide all information available about that breach.

To notify the DPO, person shall use the 'Internal report of a personal data breach' form as attached in 'Annex II' to this Privacy Policy.

14. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the CTO and/or DPO or their teams.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These rules also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD, DVD, flash drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

15. Record keeping

15.1. Records of processing activities by Nuzl as a data controller

Under the General Data Protection Regulations Nuzl is obliged to maintain a record of processing activities under its responsibility as a controller of personal data. That record contains the following information:

- the name and contact details of Nuzl and, where applicable, the joint controller and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards (if any);
- the envisaged time limits for erasure of the different categories of data;
- a general description of the technical and organisational security measures.

The record is kept in the format of "xls file" and it can be found by following the link in the 'Annex III' to this Privacy Policy. DPO is responsible for maintenance of record file, its accuracy and updating in a timely manner. CTO should inform DPO if new data appears in a system, driven by new product features, API integrations or any other means.

15.1. Records of processing activities by Nuzl as a data processor

Under the General Data Protection Regulations Nuzl is obliged to maintain a record of processing activities carried out on behalf of a controller of personal data. That record contains the following information:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards (if any);
- a general description of the technical and organisational security measures (if any).

The record is kept in the format of "xls file" and it can be found by following the link in the 'Annex IV' to this Privacy Policy. DPO is responsible for maintenance of record file, its accuracy and updating in a timely manner. CTO should inform DPO if new data appears in a system, driven by new product features, API integrations or any other means.

DPO shall ensure that records will be available to the supervisory authority on request.

16. Staff training

Every new employee before entering in his/her position in the company is obliged to read Nuzl's Privacy Policy and, where applicable, the other relevant documents depending on the extent of personal data processing activities he/she will be involved in.

Training for the new employees and annual training (at least once a year) and providing up-to-date information for all staff is very important and required by the regulator. Therefore, Nuzl has implemented its own educational programme for staff, which involves theory, materials (presentations, video presentations), practical courses and tests.

The results of training and practice will be kept and analysed by the DPO and/or CTO. At the end of every course there is a test each staff member has to take. The test for the new employees has to be taken before commencement of their duties in their position. Currently duties that face risk of data protection breaches are Human Resources, Product Development, Marketing, AML Department, Customer Support and Senior Management.

Training program includes the following topics on data protection:

- *Keeping personal information secure*. Do the staff know:
    - To keep passwords secure – change regularly, no sharing?
    - To lock / log off computers when away from their desks?
    - To dispose of confidential paper waste securely by shredding?
    - To prevent virus attacks by taking care when opening emails and attachments or visiting new websites?
    - About working on a 'clear desk' basis - by securely storing hard copy personal information when it is not being used?
    - That visitors should be signed in and out of the premises, or accompanied in areas normally restricted to staff?
    - About positioning computer screens away from windows to prevent accidental disclosures of personal information?
    - To encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen?
    - To keep back-ups of information?
- *Meeting the reasonable expectations of customers and employees*. Do the staff know:
    - To collect only the personal information they need for a particular business purpose?
    - To explain new or changed business purposes to customers and employees, and to obtain consent or provide an opt-out where appropriate?
    - To update records promptly – for example, changes of address, marketing preferences?
    - To delete personal information the business no longer requires?
    - That they commit an offence if they release customer / employee records without the consent?
    - About any workplace monitoring that may be in operation?

- *Disclosing customer personal information over the telephone*. Do the staff know:
    - To be aware that there are people who will try and trick them to give out personal information?
    - That to prevent these disclosures they should carry out identity checks before giving out personal information to someone making an incoming call?
    - To perform similar checks when making outgoing calls?
    - About limiting the amount of personal information given out over the telephone and to follow up with written confirmation if necessary?
- *Handling requests from individuals for their personal information (subject access requests).* Do the staff know:
    - That people have a right to have a copy of the personal information you hold?
    - How to recognise a subject access request?
    - Who to pass it to if it is not their responsibility to answer?
    - Time limits to respond?
    - That they may need to check the identity of the requester?
    - What to do if other people's information is contained in the proposed response?

In addition, we permanently monitor personal data protection legislation and news which will help Nuzl stay current with the changing requirements and findings. This will help the company further to keep all staff fully informed on regulatory requirements and the new data protection insights.

Request for Access to Personal Data

Notes for Applicants:

(i) Access to Personal Data

You have the right to request a copy of your personal data under the Privacy Policy.

(ii) What is personal data?

Personal data can be described as any information about you such as your name, address or telephone number. It can also be the things like what services we provide to you. It can be held in different ways, either electronically or on paper.

(iii) What is a valid request?

A valid request will have two things:

1. A description in writing of the personal data you wish to receive, including the relevant dates or names of people involved (if known). Further guidance is on the form.

2. A copy of identification material such as a passport, driving licence or two utility bills within the last three months, that will satisfy us as to your identity.

(iv) If you are applying on behalf of child

You may apply on behalf of a child if you have parental responsibility / legal guardianship. Proof of parental responsibility / legal guardianship must be provided. Please bear in mind that if the child is considered mature enough to understand their rights we will respond to the child rather than the parent.

(v) If you are applying on behalf of someone else

Where the information is requested on behalf of others e.g. a solicitor acting on behalf of their client, we need to ensure we have the data subject's consent from the solicitor to obtain the information on their behalf. Written consent or general power of attorney is required when acting on behalf of others. It is the third parties' responsibility to provide evidence for this entitlement.

(vi) Time to respond

We have to respond with 1 month from the day we receive a valid request. However, if the request is not clear enough, there is a very large amount of information, this can delay the response. If this happens, we will contact you to explain any delay. We may also ask you for more detail to help us find the information you requested.

(vii) Will I get everything I asked for?

There are several reasons why some information may be blocked out (redacted), for example it may refer to somebody other than yourself, so this will not be part of your personal information.

(viii) Fee tariff

We will provide a copy of the information free of charge. However, we can charge a 100 EUR when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Please complete the following form and sign the accompanying declaration and submit, with your proof of identity, to Nuzl Data Protection Officer at the address given below.

1. Details of person requesting the information	
Full name:	
Address:	
Tel. No:	
Email address:	

2. Are you the data subject?
☐YES: If you are the data subject please supply evidence of your identity, i.e. driving licence, passport, national identity card or photo-pass, a recent letter or bill from a utility company as evidence of address, and a stamped addressed envelope for returning the document (Please go to question 4)
☐NO: Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. If not, what other legal justification have you for obtaining access to the data? (Note that appropriate identification as above must be provided also.) (Please go to question 3)

3. Details of the data subject (if different from 1)	
Full name:	
Address:	
Tel. No:	
Email address:	

4. Please describe the information you seek together with any other relevant information. This will help to identify the information you require. Please tick the category into which your enquiry falls:		
☐Data revealing racial or ethnic origin ☐Political opinions ☐Religious or philosophical beliefs ☐Trade union membership ☐Sex life data ☐Sexual orientation data	☐Gender reassignment data ☐Health data ☐Basic personal identifiers, e.g. name, contact details ☐Identification data, e.g. usernames, passwords ☐Economic and financial data, e.g. credit card numbers, bank details	☐Official documents, e.g. driving licences ☐Location data ☐Genetic or biometric data ☐Criminal convictions, offences ☐Other

5. Detailed description of information required:

Declaration 1: To be completed where the data subject is the applicant

I can confirm that I am the Data Subject and not someone acting on his or her behalf. I can confirm that the information given on this form is correct to the best of my knowledge. Please send me the information I am entitled to under section (2) of the General Data Protection Regulation.

Signature of data subject: _____

Name: _____

Date: _____

Or

Declaration 2: To be completed where the application is being made by a third party

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the personal data referred to in this request, under the terms of the General Data Protection Regulation.

Please tick appropriate box:

□I have been asked to apply on behalf of the data subject and attach their written authorisation or general power of attorney

□I am the data subjects parent/legal guardian (with parental responsibility)

Signature of representative: _____

Name: _____

Date: _____

Please return the completed form and enclosures to the Data Protection Officer to:

Email: dpo@hexn.io

Post: Beachmont Business Centre, Suite 379, Kingstown,

Saint Vincent and the Grenadines

Documents which must accompany this application:

- evidence of your identity;
- evidence of the data subject's identity (if different from above); and

- authorisation from the data subject to act on their behalf (if applicable).

Internal report of a personal data breach to DPO

Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If this information will be needed it'll be asked for later.

About the breach

What has happened?

Tell as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

☐ Yes

☐ No

☐ Don't know

How did you find out about the breach?

When did you discover the breach?

Date: _____

Time: _____

When did the breach happen?

Date: _____

Time: _____

Categories of personal data included in the breach (tick all that apply)

☐ Data revealing racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Sex life data

☐ Sexual orientation data

☐ Gender reassignment data

☐ Health data

□Basic personal identifiers, e.g. name, contact details

□Identification data, e.g. usernames, passwords

□Economic and financial data, e.g. credit card numbers, bank details

□Official documents, e.g. driving licences

□Location data

□Genetic or biometric data

□Criminal convictions, offences

□Not yet known

□Other (please give details below)

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

□Employees

□Contractors, volunteers

□Third party vendors, suppliers, partners

□Customers or prospective customers

□Children

□Vulnerable adults

□Not yet known

□Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach.

Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

☐ Very likely

☐ Likely

☐ Neutral - neither likely nor unlikely

☐ Unlikely

☐ Very unlikely

☐ Not yet known

Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

☐ Yes

☐ No

☐ Don't know

(Cyber incidents only) If you answered yes, please specify

(Cyber incidents only) Impact on Nuzl

☐ High - you have lost the ability to provide all critical services to all users

☐ Medium - you have lost the ability to provide a critical service to some

☐ Low - there is a loss of efficiency, but you can still provide all critical services to all users

☐ Not yet known

(Cyber incidents only) Recovery time

☐ High - you have lost the ability to provide all critical services to all users

☐ Supplemented - you can predict your recovery time with additional

☐ Extended - you cannot predict your recovery time, and need extra resources

□Not recoverable - recovery from the incident is not possible, eg sensitive data has been shared publicly

□Not yet known

If there has been a delay in reporting this breach, please explain why

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training.

Have you told data subjects about the breach?

□Yes, we've told affected data subjects

□We're about to, or are in the process of telling data subjects

□No, they're already aware

□No, but we're planning to

□No, we've decided not to

□We haven't decided yet if we will tell them or not

□Something else (please give details below)

About you

Organisation name

Registered organisation address

Person making this report

In case DPO needs to contact you about this report

Name: _____

Position in company: _____

Email: _____

Phone: _____

Sending this form

Send your completed form to dpo@hexn.io with 'DPA breach notification form' in the subject field.

Annex III. Controller's processing activities records

Link to cloud service or description for your employees where the records can be found

Annex IV. Processor's processing activities records

Link to cloud service or description for your employees where the records can be found

To: Nuzl SVG LLC

Beachmont Business Centre, Suite 379, Kingstown,

Saint Vincent and the Grenadines

Declaration of Staff/Contractors/Volunteers *(choose relevant)*

I confirm that:

- I have read, understood and will comply with the firm's Privacy Policy and supplementary documents and procedures in relation to it.
- I understand my duty to comply with the EU General Data Protection Regulation, Nuzl's Privacy Policy and any instructions given by the Nuzl as the data controller and will fulfil my obligations in this area.
- I am aware of the prohibition on making any disclosure of personal data to third parties without the controller's approval.

I undertake:

- To take all possible steps to preserve strict confidentiality regarding any information to which I have access through my work.
- Never to pass any information obtained as part of the Employment Agreement/Contract for Services *(choose relevant)* to anyone outside the Nuzl team.
- To keep all names, contact details and personal data information secure.

Signature: _____

Name: _____

Date completed: _____

To: Nuzl SVG LLC

Beachmont Business Centre, Suite 379,

Kingstown, Saint Vincent and the Grenadines

Date:

Declaration of acceptance of Personal Data Protection requirements by Individual Contractor/ Volunteer/etc. (choose relevant)

I, the undersigned, confirm that:

1. I have read, understood and will comply with the Nuzl's Privacy Policy, supplementary documents and procedures in relation to it.
2. I understand my duty to comply with the EU General Data Protection Regulation, Nuzl's Privacy Policy and any instructions given by the Nuzl as the data controller and will fulfil my obligations in this area.

I, the undersigned, acknowledge, understand and agree to adhere to the following conditions of access to all information at Nuzl group:

1. I will maintain the confidentiality and security of all of Nuzl group's information including personal data in possession of Nuzl group as a controller and I understand that unauthorised disclosure of any information may be an invasion of privacy and may result in disciplinary, civil, and/or criminal actions against me.
2. I will process the personal data only on documented instructions from the Nuzl as a controller, including with regard to transfers of personal data to a third country or an international organisation.
3. I will not disclose any personal data information to anyone other than those to whom I am authorised to do so.
4. Should I be granted access to Nuzl group's electronic systems, I understand that my Username is considered equivalent to my signature, and I am responsible for all activity conducted under my Username.
5. I will only access the Nuzl's information for the purposes for which I am explicitly authorised. I will not use Nuzl group's information, including personal data or confidential information, for my personal interest or advantage or any other business purposes.
6. I will, at the choice of the Nuzl as a controller, delete or return all the personal data to the Nuzl after the end of the provision of services relating to the Contract of Services, and I will confirm, in writing, that no copies have been made or left in my possession.
7. Once my contract is completed with Nuzl, I understand that I will continue to be bound by this signed declaration of acceptance.

Signature: _____

Name: _____