

Data Protection Policy

The information contained in this document is highly sensitive and is protected by laws and regulations. Unauthorised disclosure or use of this information may result in legal action and other consequences. Employees are expected to maintain the confidentiality of this document and use the information only for legitimate business purposes within the scope of their duties.

Document information

Subject	Data Protection Policy
Purpose	This document sets out the strategy of the Company to comply with applicable data protection regulations, requirements, and best practice and in line with the Company's risk appetite and the risk assessment of the business. This policy is designed to assist the best practice for privacy policies for Duelbits.com.
Involvements	All departments relevant to privacy management efforts across the Company, including: • Legal and Compliance Team • Information Security Team
Responsibility	Head of Compliance, Head of Security
Approval	Head of Compliance, Board of Directors
Review	Normally on an annual basis or earlier as needed
Classification	Confidential

Version history

Date	Version	Author	Summary of changes
April 2022	1.0	Legal and Compliance team	Creation
September 2023	2.0	Legal and Compliance team	Annual review
July 2023	3.0	Legal and Compliance team	Annual review

Table of contents

1. Introduction/Purpose of this Policy	4
2. Scope and applicability	4
3. Principles	5
4. Data Protection Officer	5
5. Collection, Use and Disclosure of Personal Data	6
6. Personal data collection and personal data examples	7
7. Consent Obligation	9
8. Purpose Limitation Obligation	10
9. Notification Obligation	10
10. Data Quality	11
11. Protection Obligation	11
12. Retention Obligation	11
13. Transfer Limitation Obligation	12
14. Access and Correction	13
15. Data Breach Notification	13
16. Data Portability	14
17. Contacting Data Protection Officer	14
18. Review of this Policy	14

1. Introduction/Purpose of this Policy

- 1.1. **Liquid Entertainment N.V. (hereinafter “Company”, “Duelbits”)**, is a company duly incorporated under the laws of Curacao under the register number 153298 with its registered address Zuikertuintjeweg z/n (Zuikertuin Tower), Willemstad, Curaçao. It provides consumer-facing entertainment and gaming products with support of digital the Company holds a gaming licence issued by the government of Curacao and operates the online casino www.duelbits.com under the licence GLH-OCCHKW076092020.
- 1.2. The Company is committed to meet the highest industry standards and regulations under the laws of Curacao pertaining to personal data protection and other jurisdictions that the Company operates, to ensure security in the processing of personal data in order to protect individuals’ personal data.
- 1.3. The purpose of the Policy is to set forth the requirements and standards for the protection of personal data regarding the collection, usage, transfer, disclosure and care of personal data. Personal data applies to data stored in electronic and non-electronic formats.
- 1.4. Herein the Policy, “Personal Data” refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which The Company has or is likely to have access, including data in our records as may be updated on an ongoing basis.
- 1.5. Examples of such Personal Data an individual may provide the Company include name (including any aliases), unique identification number, contact details, residential address, government-issued document, and any other information relating to the individual or any individuals which are provided to the Company.

2. Scope and applicability

- 2.1 This Policy applies to all Company’s staff employed, whether temporary, contractual-term, fixed-term, or permanent, or engaged by the Company and any related entities, as well as any outsourced personnel, as applicable.
- 2.2 If some local regulations or operational requirements require any deviations from the Company level policy, these requirements will be tracked in The Company’s policy dispensation tracker and will require approval by the Audit, Risk and Compliance Committee.
- 2.3 This Policy has been reviewed and approved by the Head of Compliance and the Board of Directors.

2.4 This Policy should be updated at least annually or upon any material change to the Company's profile or strategy, or changes/updates to the applicable laws or regulations in relevant jurisdictions.

2.5 Questions or concerns regarding this Policy or record keeping should be directed to the Head of Compliance. Unless explicitly stated otherwise, any exceptions to the requirements set out in this Policy must have the prior approval of the relevant or Head Compliance.

3. Principles

3.1 The principles underpinning the Company's approach to data protection requirements and practices are as follows:

- To develop and implement policies and processes for data protection that satisfy the regulatory obligations in the jurisdictions that The Company operates in;
- To safeguard Personal Data from misuse and to maintain individuals' trust in the Company to manage their data;
- To protect fundamental rights and freedoms of individuals and in particular their right to the protection of Personal Data within the relevant laws and regulations.
- To develop a process to receive and respond to complaints with respect to the application of the required laws and regulations and;
- To make information available on request on the data protection practices and complaints process by relevant regulators.

4. Data Protection Officer

4.1 The Company will designate the General Counsel as the Data Protection Officer.

4.2 The roles and responsibilities of the Data Protection Officer includes:

- Ensure that the Company and the entities associated with the Company process the personal data in compliance with the relevant laws and regulations;
- Responsible for handling and investigating queries or complaints;
- The Data Protection Officer can delegate this responsibility to a dedicated individual or team;
- Provides advice and recommendations to The Company and the entities associated with the Company about the interpretation or application of data protection requirements;
- Cooperate with relevant authorities regarding requests, complaint handling, inspections, and other matters;
- Regular reporting to the Senior Management;

- Escalate to the Audit, Risk and Compliance Committee, Senior Management and the Board, where appropriate, on any material concerns / issue;
- The Data Protection Officer with the employees in the Company have shared responsibility and accountability for the protection and confidentiality of Personal Data.

5. Collection, Use and Disclosure of Personal Data

5.1 The Company requires to collect Personal Data from individuals that include customers, business partners, contractors, and other individuals in accordance with the relevant laws and regulations.

5.2 The Company considers “reasonableness” in the collection, use and disclosure of Personal Data that is appropriate in the circumstances from the perspective of the individual.

5.3 The Company may also collect, use and disclose unsolicited Personal Data such as Person Data received by The Company where the Company has taken no active steps to collect such information.

5.4 Where the Company receives unsolicited Personal Data, it will decide whether it could have collected the information as a substitute for reasonably collected required information.

5.5 The Company collects Personal Data when it is necessary for business and regulatory purposes or to meet the purposes for which the individuals have submitted the Personal Data.

5.6 Where any Personal Data relating to a third party individual is provided to the Company, the individuals represent and warrant that they have obtained the necessary consent of the third party to provide us with their Personal Data for the respective purposes.

5.7 The Company requires that all Personal Data submitted to the Company is complete and accurate.

5.8 The Company, generally, collects, uses and discloses Individuals’ Personal Data for the following primary purposes:

- To provide our products and services;
- To respond to the individual’s request, feedback, complaints and queries for the purposes for which it was provided to us
- For identification and verification purposes;
- To maintain ongoing business relations;
- To inform customers and other contacts of the products and services we offer, news and developments, promotional campaigns and other business-related activities that may be of interest to them;

- To prevent, detect, investigate and report financial crime and other serious crime;
- For regulatory and reporting purposes, to comply with relevant laws and regulations;
- For protecting and enforcing our contractual and legal rights and obligations in connection with any claims, actions or proceedings; and
- All other purposes related to the business

5.9 The Company may also use or disclose existing data for secondary purposes that may differ from or related to the primary purposes for which the Company had originally collected the Personal Data. If the Personal Data is sensitive information, the secondary purpose must be related to the primary purpose.

5.10 In the use or disclose existing data for secondary purposes, The Company may rely on deemed consent by notification.

5.11 The Company does not disclose Personal Data to anyone including third parties except when required by laws and regulations, when we have the individual's consent or deemed consent or in cases where we have engaged third parties specifically to assist with our Group's activities. Third parties whom we engage will be bound contractually to ensure all information are secured and kept confidential.

5.12 The Company, however, will disclose Personal Data on the following premise:

- Individual's consent;
- Regulatory request; or/and
- Required by the laws and regulations to disclose the information.

6. Personal data collection and personal data examples

6.1 Personal Data may be collected in the following manners (non-exhaustive):

- When individuals submit an application via mobile application or website relating to account opening relating to the use of our products and services;
- When individuals enter into any agreement or/and provide other documentation or information in respect of your application and interactions with us when the individuals use our services;
- When individuals interact with our customer support (e.g. via emails, mobile or our website);
- When individuals use our products and services;
- When establishing relations with individuals (e.g. third party vendors) to subscribe to their products and services;

- When individuals request that we contact them or include them in an email or mailing list;
- When we receive references from individuals, business partners or third parties;
- When individuals respond to our promotions, campaigns or to any additional requests for Personal Data; and/or
- When individuals are contacted by and respond to, our customer support

6.2 We may collect the following categories of Personal Information submitted to us when you create an account or use our Services:

- Contact information, including first and last name, email address and physical address to communicate with you directly, and to send you marketing communications in accordance with your preferences;
- Account information, including first and last name, email address, physical address, user ID profile information, account balances, payment and purchase history information, and any other information you provide to us. We use this information to administer your account, provide you with the relevant service and information, communicate with you regarding your account and your use of the Services, and for customer support purposes;
- Payment information, if you sign up for one of our Services requiring payment. We collect the information needed to facilitate such payment, including your crypto wallet information or other payment card information. We use third-party crypto and credit card payment processors to process transactions. As such, we do not retain any financial information directly in connection with crypto payments (such as credit card numbers). Rather, all such information is provided directly by you to our third-party service provider.
- Identification information, including government issued IDs and some government issued information such as tax returns etc. We use third-party identification verification service providers to collect this information directly and facilitate all identity and background checks. These providers will only process this information to provide us with the identity verification and background check services. Additional privacy information may be made available to you by the third parties at the time your information is collected;
- Inquiry and communications information, including information provided in custom messages sent through the forms, in chat messages, to one of our email addresses, or via phone. This also includes contact information provided on our Services. We use this information to investigate and respond to your inquiries, and to communicate with you, to enhance the services we offer to our users, and to manage and grow our organization;
- Newsletter and promotional messages, including email address and applicable interests and communication preferences. We use this information to manage our communications with you and send you information about products and services we think may be of interest to you. If you are a creator, we may also contact you with information about your

account, your audience, your activities, or your payments. If you wish to stop receiving promotional email messages from us, simply click the “unsubscribe link” provided at the bottom of the email communication. You will not be able to unsubscribe from certain services-related email communications (e.g., account verification, confirmations of transactions, and technical or legal notices);

- Contest, and survey information, including information provided when you enter a contest or sweepstakes, or information included in any questions submitted through surveys or content of any testimonials. We use this information to administer and facilitate the Services, to respond to your submission, to communicate with you, to conduct market research, to inform our marketing and advertising activities, and to improve and grow our business;
- Event and webinar information, including registration information, call-in details, attendee badge information, and contact information. We use this information to administer and facilitate the Services and improve and grow our business;
- Information collected through the use of the Services, including any files, documents, , data, records or information you choose to upload or transmit through your communications with us or your use of the Services.
- Feedback information, including feedback and ratings you provide relating to the Services. We use this information to communicate with you, to conduct market research, inform our marketing and advertising activities and improve and grow our business.
- Personal information automatically collected: As is true of many digital properties, we and our third-party partners may automatically collect certain information from or in connection with your device when visiting or interacting with our Services, such as the list below and in the sub-sections here:
- Log data, including internet protocol (IP) address, operating system, device type and version, browser type and version, browser ID, the URL entered and the referring page/campaign, date/time of visit, other user agent string data, the time spent on our Services, and any errors that may occur during the visit to our Services. Log data may overlap with the other categories of data below;
- Analytics data, including the electronic path you take to our Services, through our Services and when exiting our Services, UTM source, as well as your usage and activity on our Services, such as the time zone, activity information (first and last active date and time), usage history (flows created, campaigns scheduled, emails opened, total log-ins) as well as the pages, links, objects, products and benefits you view, click or otherwise interact with. We may also analyze the interaction between you and your customer using our Services.
- Location data, including geolocation that we or our third-party providers may derive from your IP address.

- Cookie data, including (i) cookies or small data files that are stored on an individual's computer and (ii) other, related technologies, such as web beacons, pixels, embedded scripts, location-identifying technologies, and logging technologies (collectively, "cookies") to automatically collect this personal information. We may also use this information to distinguish you from other users of our Services. This helps us monitor and analyse how you use and interact with our Services. It also helps us and our partners to determine products and services that may be of interest to you. For more information about these practices and your choices regarding cookies, please see the "Control over your information" section below.

7. Consent Obligation

7.1 The Company is required to obtain the consent of the individual before the collection, use or disclosure of Personal Data for respective purposes outlined in this Policy.

7.2 The Company will consider the individual is deemed to consent to the collection, use or disclosure of Personal Data for a purpose if:

7.3 The individual, without actually giving consent, voluntarily provides Personal Data to the organization; and

7.4 It is reasonable that the individual would voluntarily provide the data.

7.5 The Company will allow the individual to withdraw consent permitted by the relevant laws and regulations, with reasonable notice, and inform him/her of the likely consequences of withdrawal. Once consent is withdrawn, The Company will cease to collect, use or disclose the individual's Personal Data to the extent permitted by the relevant laws and regulations.

7.6 The Company may collect Personal Data about the individual, without the consent of the individual or a source other than the individual, in circumstances or for the purposes, and subject to any condition in relation to the following:

- Vital interests of individuals.
- Matters affecting public;
- Legitimate interests;
- Business assets transactions;
- Business improvement purposes; or
- Disclosure by a public agency or the use of Personal Data by the Company is consistent with the purpose of the disclosure by the public agency

7.7 The Company may use and disclose Personal Data about the individual, without the consent of the individual, in circumstances or for the purposes, and subject to any condition in relation to the following:

- Vital interests of individuals;
- Matters affecting public;
- Legitimate interests;
- Business assets transactions;
- Business improvement purposes;
- Public interest; or
- Research

8. Purpose Limitation Obligation

8.1 The Company will collect, use or disclose Personal Data for the purposes that a reasonable person would consider appropriate under the given circumstances and for which the individual has given consent.

8.2 The Company may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his/her Personal Data beyond what is reasonable to provide that product or service.

9. Notification Obligation

9.1 The Company will notify the individuals of the purposes for which the Company is intending to collect, use or disclose Personal Data at the point or before collection of such information.

9.2 Upon request, the Company will notify the individuals, about the collection, use or disclosure of the Personal, in accordance with applicable laws and regulations.

9.3 Where The Company requires to collect Personal Data about an individual from another organization without the consent of the individual, The Company will provide sufficient information regarding the purpose of the collection to enable the other organization to determine the disclosure.

9.4 The Company will not be required to notify the individual if it is deemed to have consented to the collection, use or disclosure.

10. Data Quality

10.1 The Company will take reasonable steps to ensure that the Personal Data it collects is accurate, up-to-date and complete.

10.2 The Company will take reasonable steps to ensure that Personal Data it uses or discloses is, in relation to the purpose, accurate, up-to-date, complete and relevant.

11. Protection Obligation

11.1 The Company will develop and implement measures to ensure security and protection of Personal Data in our possession or control to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

11.2 The Company has established Information Security Policy and implemented the requirements set within the said policy to ensure the security and protection of information security systems including data. Please refer to the Information Security Policy for more details.

11.3 All employees with access to personal identifiable information (“PII”) are required to agree to confidentiality of such information or sign some other form of confirmation e.g. confidentiality as part of employment contract.

12. Retention Obligation

12.1 The Company will retain Personal Data as long as it is reasonably necessary to comply with legal and regulatory requirements. Please refer to The Company Record-Keeping Policy for more details on the requirements.

12.2 The Company will cease to retain Personal Data, as soon as it is reasonable that the purpose for collection of such Personal Data is no longer necessary for legal and regulatory requirements.

12.3 If the Company collects unsolicited Personal Data where such information is also contained in Government records, The Company will not be required to destroy or de-identify such information and will handle and process it in accordance with the Policy.

12.4 However, the Company will destroy or de-identified as soon as practicable if it is lawful and reasonable to do so.

12.5 if your personal information is subject to the EU GDPR or UK GDPR, the criteria used to determine the period for which personal information about you will be retained varies depending on the legal basis under which we process the personal information:

- Contract. Where we are processing personal information is based on contract, we generally will retain your personal information for the duration of the contract plus some additional limited period of time that is necessary to comply with law or that represents the statute of limitations for legal claims that could arise from our contractual relationship.
- Legitimate interests. Where we are processing personal information based on our legitimate interests, we generally will retain such information for a reasonable period of time based on the particular interest, taking into account your fundamental interests and your rights and freedoms.

- Consent. Where we are processing personal information based on your consent, we generally will retain your personal information until you withdraw your consent, or otherwise for the period of time necessary to fulfil the underlying agreement with you or provide you with the applicable service for which we process that personal information.
- Legal obligation. Where we are processing personal information based on a legal obligation, we generally will retain your personal information for the period of time necessary to fulfil the legal obligation.
- Legal claim. We may need to apply a “legal hold” that retains information beyond our typical retention period where we face threat of legal claim or intent to establish a claim. In that case, we will retain the information until the hold is removed, which typically means the claim or threat of claim has been resolved.
- In all cases, in addition to the purposes and legal bases, we consider the amount, nature and sensitivity of the personal information, as well as the potential risk of harm from unauthorized use or disclosure of your personal information.

13. Transfer Limitation Obligation

13.1 Subject to section 13.2, the transfer of any Personal Data to territory outside of the Company or territory outside of entities associated with The Company is permitted in accordance with the respective local laws and regulations.

13.2 International transfers of your personal information. The personal information we collect may be transferred to and stored in countries outside of the jurisdiction you are in where we and our third party service providers have operations, including in the United States. If you are accessing our Services from the European Economic Area (“EEA”), UK, Switzerland or any other jurisdictions, your personal information will be processed outside of the EEA, the UK and Switzerland.

13.3 In the event of such a transfer, we will ensure that: (i) the personal information is transferred to countries recognised as offering an equivalent level of protection to that of the EEA ; or (ii) the transfer is made pursuant to appropriate safeguards, such as standard contractual clauses adopted by the European Commission. If you wish to enquire further about these safeguards used, please contact us using the details set out at the end of this Privacy Notice.

13.4 The Company will take appropriate steps to ensure that the recipient of the Personal Data will not breach any relevant laws and regulations.

14. Access and Correction

14.1 Upon request, the Company will provide the individual with access to his / her Personal Data and other appropriate information on his / her Personal Data in compliance with the relevant laws and regulations.

14.2 However, the Company will not provide an individual with Personal Data or other information if it is in relation to the following:

- Threaten the safety or physical or mental health of an individual other than the individual who made the request;
- Cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- Reveal Personal Data about another individual;
- Reveal the identity of an individual who has provided Personal Data about another individual and the individual providing the Personal Data does not consent to the disclosure of his / her identity; or
- Be contrary to the national interest.

14.3 The Company will ensure that the individual is not informed / notified about any disclosure of Personal Data about the individual to a law enforcement agency.

14.4 Upon request, the Company will correct an error or omission in the individual's Personal Data that is in the Company possession or control within 30 days.

15. Data Breach Notification

15.1 If The Company identifies a data breach and that the likelihood and impact of it will result in significant harm to individuals and/or are of significant scale, The Company will notify the relevant authorities and affected individuals as soon as practicable.

15.2 Such incidents must be escalated to the Head of Security and Head of Compliance to initiate investigation and develop an appropriate response plan. The respective executives shall be notified as deemed appropriate and in accordance with the escalation process.

15.3 As part of the incident response procedure, a description of the nature, cause, and timing of the data breach should be determined during the internal identification process. Assessment of the risks to the individuals concerned. The cause(s), process failures, of the breach and the individual(s) responsible.

15.4 Significant scale of breach includes involving Personal Data of 500 or more individuals. Such that if The Company is unable to determine the actual number of individuals but has reason to believe to be at least 500, the Company will notify the relevant authorities and subsequently update the relevant authorities when the actual number is established.

15.5 When the Company determines that the breach is notifiable to the relevant authorities, it will notify as soon as practicable, but no later than 3 calendar days. For the benefit of the doubt, the time frame to

notify the relevant authorities and/or affect individuals commences from the time The Company determines that the data breach is notifiable.

16. Data Portability

16.1 Upon request, The Company may transmit the individual's data in our possession or control to another organization in a commonly used machine-readable format. This format should be emphasised across all the departments and should be confirmed. This will be able to incorporate into the process of portable data and ensure.

17. Contacting Data Protection Officer

17.1 The business contact information of the Data Protection Officer is DPO@easygo.io has been established to make available to the public should any individual have any concerns, queries, problems or complaints about Personal Data or our handling of Personal Data.

17.2 The Company will establish a process to:

- Communicate with the individual to acknowledge receipt of any concerns, queries, problems or complaints, and obtain sufficient information from the individual;
- Investigate and analysis;
- Escalate and report to Senior Management and/or Board of Directors, where appropriate; and
- Communicate the outcome of the investigation to the individual.

18. Review of this Policy

18.1 This Policy may be updated from time to time. If any changes are made to this Policy the Company will inform the (if needed) in advance by email, notice on the website or other agreed communications channels. Notice may consist of posting such changes on our website or by other means in accordance with applicable laws.

18.2 The Company will endeavour to communicate the changes to the customers in advance, giving an appropriate amount of time to understand the changes before they become effective and give the opportunity to customers to consent to any changes prior to accessing the services.