

Terms of Use, Privacy & Security

I. Terms of Use

1. Registration
2. User Content
3. User's Limited License for Use
4. User's Limited License of Content
5. Intellectual Property
6. Remedies for Terms of Use Violations
7. Errors and Corrective measures
8. Termination of User Access
9. Communications
10. Privacy and Security
11. Changes to the Terms of Use
12. Entire Agreement
13. Governing Law and Jurisdiction

II. Privacy

1. Information collection
2. Information Usage
3. Navigational Information
4. Opting Out and Unsubscribing
5. General Data Protection Regulation
6. Data Processing and Protection Agreement
7. Data Centres
8. Logging

III. Security

1. General Security Agreement
2. Security Measures
3. Network Security

PLEASE READ THIS CAREFULLY.

These Terms of Use are entered by and between you and bugle, S.A., and together with the Privacy and Security Policies govern your access to bugle.app and subdomains managed by bugle, S.A. (“Sites”), as well as any content or functionality of the services, as a registered user (“User”).

Bugle provides a video training and informal knowledge sharing platform designed for organizations to deliver video training and other forms of digital content, which enables Users authorized by bugle customers (“Customers”) to engage with Customers or third parties digital content through the Sites.

The content on the Sites, including all data, information, software, technology, marks, logos, designs, text, graphics, pictures, audio and video files, other data or copyrightable materials or content, and their selection and arrangement, is referred to herein as "Content." Content uploaded, transmitted, or posted by Users, whether they are Instructors or Students, is referred to herein as “User Content.”

Your use of the Sites and/or the Content contained therein constitutes your agreement to be bound by these terms of use. The Sites and Content are offered to you conditioned on your acceptance of these Terms of Use and all terms, conditions, and notices contained herein. Please read the Terms of Use carefully before you start to use the Sites. By using the Sites, you accept and agree to be bound and abide by these Terms of Use and our Privacy and Security Policies, incorporated herein. If you do not want to agree to these Terms of Use or the Privacy Policy, you must not access or use the Sites.

If you have questions regarding these Terms of Use, Privacy and Security Policies, please contact us at:

BUGLE, S.A.

Av. Eng.º Duarte Pacheco,

Amoreiras, Torre 2, 16.º-A,

1070-102 Lisboa, PORTUGAL

Email: hello@bugleteam.com

I. Terms of Use

1. Registration

To use bugle you will need to register and obtain a password-protected account. You agree to provide accurate and complete information when registering and always thereafter. You are solely responsible for maintaining the confidentiality of your account, username, and password, and for all activities associated therewith. Please contact us at hello@bugleteam.com if you suspect your account was compromised or was used without your permission, and promptly take steps to secure your account.

2. User Content

User Content is and remains that User's property, and Bugle's only right to that User Content is the limited licenses to it granted in these Terms of Use. The Sites, and all Content other than User Content and all software available on the Sites or used to create and operate the Sites, is and remains the property of bugle or its Customers.

All trademarks and service marks, whether registered or unregistered, as well as product names and company names or logos, displayed or mentioned on the Sites are the property of their respective owners.

3. User's Limited License for Use

Bugle grants you a limited, non-exclusive license to access and use the Sites for your own personal purposes. This license is personal to you and may not be assigned or sublicensed to anyone else. Except as expressly permitted by bugle in writing, you will not reproduce, redistribute, sell, create derivative works from, decompile, reverse engineer, or disassemble the Sites and Content.

4. User's Limited License of Content

Bugle grants to Users a limited, revocable, non-exclusive, non-sublicensable license to access the Sites and to view, copy, and print the portions of the Content available to Users on the

Sites. This includes access and use of the Courses and content provided therein. Such license is subject to these Terms of Use, and specifically conditioned upon the following:

- Users may only view, copy, and print such portions of the Content for their own use;
- Users may not modify or make derivative works of the Sites or Content, or reproduce, distribute, or display the Sites or any Content except as expressly permitted in these Terms of Use;

5. Intellectual Property

The Sites and their entire features and functionality are owned by bugle, its licensors, or other providers of such material and are protected by Portuguese and international copyright and trademark.

Users may not engage in any activity on or through the Sites, including transmitting or using User Content, that infringes or otherwise makes unauthorized use of another party's copyright, trademark, or other intellectual property or proprietary rights.

6. Remedies for Terms of Use Violations

Bugle reserves the right to seek all remedies available at law and in equity for violations of these Terms of Use, including but not limited to the right to block access from a IP address or other user identifier to the Sites.

7. Errors and Corrective measures

Bugle does not warrant that the Sites offered through the Sites will be error-free or otherwise reliable, free of viruses, or other harmful components. Bugle may make improvements to the Sites and their features and functionality at any time and will use best efforts to avoid disrupting peak hours, though some downtime may occur.

8. Termination of User Access

Bugle may discontinue any User or visitor's participation in the Sites at any time.

9. Communications

Bugle may notify Users of relevant information regarding the Sites and Content (a) by emailing Users at the contact information they provide in their account registration, or (b) by posting the notice elsewhere on the Sites.

10. Privacy and Security

Your use of the Sites is subject to our Privacy and Security Policies.

11. Changes to the Terms of Use

Bugle may review and update these Terms of Use at any time. All changes will be communicated to you and apply to all access to and use of the Sites thereafter. Your continued use of the Sites following the communication of revised Terms of Use is contingent to your acceptance and agreement to the changes.

12. Entire Agreement

If any provision of these Terms of Use is deemed unlawful or unenforceable by a court of law, that provision shall be deemed severed and shall not affect their validity and enforceability.

13. Governing Law and Jurisdiction

These Terms of Use are governed by and construed in accordance with the internal law of Portugal. Any action arising out of or relating to these Terms of Use shall be filed only in the courts of Portugal.

II. Privacy

1. Information collection

1.1 General bugle Platform Usage

The user of the bugle platform may be asked to provide personal information in order to, but not restricted to, confirming login credentials and access permission. The customer may allow or decline the user's access and permissions. When using bugle, navigational and usage information is collected, and made available in report format to bugle platform administrators – both customer and bugle staff with reporting permissions.

1.2 "Personal Information" means any information the bugle platform users voluntarily provide about themselves. This information may include but is not restricted to name, email address, company name, job title.

1.3 "Navigational Information" means information about the user's usage of the bugle platform. This information includes but is not restricted to the user's course attendance and interaction with any available content, the user's IP address, browser information, geographical location, pages visited and length of visit. The usage of this information is detailed on clause 2.4 ("Navigational Information Usage") and 3 ("Navigational Information").

2. Information Usage

2.1 bugle uses the information collected in the bugle platform in compliance with this privacy policy.

2.2 bugle does not share or sell to third parties the bugle platform users' personal information.

2.3 the information collected from bugle platform users is used to:

- improve the users' experience on bugle platform;
- report on user's activity to understand course and other content efficacy and goals;
- send communications to users based on their usage of the platform;
- inform users of new available content.

2.4 Navigational Information Usage. Navigational information collected from bugle platform users is used to provide a better experience in the bugle platform, and for the customer to view and report on users' activities.

2.5 Security of Personal Information collected

Measures are in place to prevent unauthorized access or disclosure of bugle users' personal information, including technological security measures and safety procedures. For queries regarding the security of personal information, contact hello@bugleteam.com.

2.6 Retention of Personal Information

Bugle retains Personal Information that bugle users provide for as long as the customer maintains business relationship with bugle, or as needed to comply with legal obligations, resolve disputes and enforce our agreements. A bugle user can request the customer or bugle to have their personal information deleted as described in clause 4 ("Opting Out and Unsubscribing").

3. Navigational Information

3.1 Cookies. bugle uses cookies to collect information about bugle users, to allow for login sessions and to analyse usage and track users' platform navigation.

3.2 Log Files. Bugle collects demographic information and computer hardware and software information using log files not associated with the users' personal information. This information includes, but is not limited to IP address, browser, operating system, files viewed on the platform, access times. Bugle uses this information to measure and analyse bugle platform statistics.

4. Opting Out and Unsubscribing

4.1 Reviewing, Correcting and Removing Personal Information. Upon request the customer or the user bugle will provide the users information about their personal information collected by bugle, and to:

- review the user personal information collected;
- request the correction of errors, outdated information, or omissions in user information;

- request the opt out and cease of contact;
- request that user information is deleted from bugle records.

4.2 To exercise these rights, the user should contact the customer or bugle at hello@bugleteam.com. The bugle team will contact and provide information to the customer on how to respond to the users' requests to change, correct, or delete their information within a reasonable timeframe and notify the user the action has been taken.

4.3 Unsubscribe from bugle platform Communications. Users may unsubscribe from bugle notifications by contacting the customer or sending an email with such solicitation to hello@bugleteam.com.

4.4 bugle platform personal information collection, usage and management is fully compliant with General Data Protection Regulation (GDPR). Any situation related to personal information management not addressed in the previous clauses, the user can refer to the GDPR (Clause 6 "General Data Protection Regulation" of I.II bugle SaaS Tool).

5. General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR) is a privacy regulation in terms of its breadth, depth, and impact. The GDPR takes effect on May 25, 2018. bugle has already undergone the necessary steps for full compliance.

6. Data Processing and Protection Agreement

6.1 bugle collects information from users for the purposes of:

- provide the services subscribed by the customer, including prevention, detection and resolution of technical and security issues;
- to respond to customer support requests;
- to fulfil the obligations under bugle Service Level Agreement (SLA) and Terms of Service

6.2 When processing users' Personal Data on behalf of our subscription services customers, bugle ensures that the provisions of this clause are fully complied with. Bugle agrees that the customer and/or its affiliates are data controllers and that bugle is a data processor of the users' Personal Data.

6.3 bugle shall only process Personal Data from Customers' users pursuant to the performance of the Services and until the date that bugle ceases to provide the Services to the Customer. On termination, upon customer request, bugle agrees to transfer the Customers' users Data (including all Personal Data) to the Customer and to subsequently deactivate and sanitize the Customers' users Data within 15 days after termination.

6.4 In providing the Services and in meeting its obligations under this Agreement, bugle undertakes to the customer that it will:

6.4.1 process Customers' Users Data in accordance with written instructions from the customer or pursuant to the performance of the Services. If bugle is required to process the Customers' users Data for any other purpose by European Union or Member State law to which bugle is subject, bugle will inform the Customer of this requirement before the processing, unless that law prohibits this on important grounds of public interest;

6.4.2 notify the customer immediately if, in bugle's opinion, an instruction for the processing of the customers' users Data given by the customer infringes Data Protection Legislation;

6.4.3 implement and maintain appropriate technical and organisational measures to protect the Customers' users Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected. As a minimum, these should include the requirements required under Data Protection Legislation.

6.4.4 not to give access to or transfer any Customers' users Data to any third party (including any affiliates, group companies or sub-contractors) without the express prior written consent of the customer. Where the customer does consent to bugle engaging a sub-contractor to carry out any part of the Services, bugle must ensure the reliability and competence of the third party, its employees and agents who may have access to the Customer Data and must include in any contract with the third party provisions in favour of the customer which are equivalent to those in this clause and as are required by Data Protection Legislation. For the avoidance of doubt, where a third party fails to enable bugle to fulfil its obligations, bugle will remain fully liable to the customer;

6.4.5 take reasonable steps to ensure the reliability and competence of bugle's personnel who have access to the Customers' users Data;

6.4.6 ensure that personnel required to access Customers' users Data are informed of the confidential nature of the personal data comprised within such data and comply with the obligations set out in this clause;

6.4.7 ensure that none of bugle's personnel publish, disclose or divulge any of the Customer or Customers' users Data to any third party unless directed in writing to do so by the customer;

6.4.8 not retain any of the customers' users Data for longer than is necessary to perform bugle's obligations under this Agreement and the Service Level Agreement, at the end of the Services upon customer's request, securely destroy or return such data to the customers' users; and

6.4.9 allow the customer and its respective auditors or authorised agents to conduct audits or inspections during the term of the Agreement and for 6 months thereafter which will include providing access to the premises, resources and bugle personnel and bugle's sub-contractors use in connection with the provision of the Services, and provide all reasonable assistance in order to assist the customer in exercising its audit rights under this sub-clause to enable verification that the customers' and customers' users Data is and/or has been processed in accordance with this Agreement and Data Protection Legislation.

6.4.10 bugle shall aid the customer into cooperation with the supervisory authorities, where necessary, including direct cooperation between bugle and such supervisory authorities.

6.5 In the event that bugle directly receives a request from a data subject to exercise one of the rights described in the Data Protection Laws (a "Data Subject Request"), bugle will:

- Notify the customer immediately of the Data Subject Request, without responding to that Data Subject Request unless it has been otherwise authorised by the customer to do so;
- Provide details of the Data Subject Request (and any other relevant information the customer may reasonably request) to the customer within three (3) business days;
- Provide such assistance to the Customer's Data Controller that they may reasonably require for the purposes of responding to the Data Subject Request.

6.6 If bugle or its contractors become aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to Customers Data (a "Security Breach"), or reasonably believe that a Security Breach has occurred, bugle will immediately notify the customer in writing and on an on-going basis will:

6.6.1 Immediately provide the customer with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach and the identity of each affected person, (as well as periodic updates to this information and any other information the customer may reasonably request relating to the Security Breach) and the name and contact details of the data protection officer or other point of contact where more information can be obtained;

6.6.2 Assist the customer and take action immediately, at bugle's own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of the Security Breach and, with the prior written approval of the customer, to carry out any recovery or other action necessary to remedy the Security Breach; and

6.6.3 within four (4) weeks of closure of the incident, provide the customer a written report describing the Security Breach, the root cause analysis, actions taken by bugle during its response and bugle's plans for future actions to prevent a similar Data Breach from occurring;

6.6.4 not release or publish any filing, communication, notice, press release, or report concerning the Security Breach (including supervisory authorities) without the customer's prior written approval (except where required to do so by law).

6.7 If the European Commission lays down, or an applicable supervisory authority adopts, standard contractual clauses for personal data processing activities and the customer notifies bugle that it wishes to incorporate any element of any such standard contractual clauses into this Agreement, bugle will agree to the changes as reasonably required by the user in order to achieve this.

6.8 bugle will not process Users Data outside the European Economic Area, or a country in respect of which a valid adequacy decision has been issued by the European Commission, except with the prior written consent of the user and subject to the adoption of the appropriate security measures in accordance with the Data Protection Laws.

7. Data Centres

bugle's products run on world class infrastructure hosted at Amazon data centres running on Amazon Web Service (AWS) technology. Our data centres are in Dublin, Ireland and data never leaves Europe. Amazon maintains security certifications with: SOC 1 / ISAE 3402; SOC 2; SOC 3; FISMA, DIACAP, and FedRAMP; CSM Levels 15; PCI DSS Level 1; ISO 9001 / ISO 27001.

Customer data is stored in multi-tenant datastores. Strict privacy controls exist in our platform code to ensure data privacy. We have many unit and integration tests in place to ensure privacy controls work as expected.

8. Logging

Logging is used extensively for platform troubleshooting and investigating issues. Logs are streamed in real time and over secure channels to a centralized logging service. This also allows bugle technical support and development teams to view logs without gaining access to the production systems.

III. Security

1. General Security Agreement

1.1 bugle will:

1.1.1 use up-to-date, commercially available firewalls, anti-virus software and virus detection software designed to prevent and detect the introduction of a virus to any software or computer system related to the SaaS Service;

1.1.2 take all precautions necessary to preserve the integrity of User Data and to prevent any loss, corruption, disclosure, theft, manipulation or interception of the Customer Data, and

1.1.3 make secure back-up copies of the User Data.

1.2 If any user signs up to become a registered User, the user will have to provide a set of information required by bugle and may also be asked to choose a username and a password for their account.

1.3 the User agrees to provide true, accurate, current and complete information to bugle in connection with any use or access of the SaaS Services and will maintain and update this information to keep it true, accurate, current and complete. bugle reserves the right to terminate a specific user's use of the Service in the event we learn or believe any information provided may be false, inaccurate, not current or incomplete.

1.4 the user is responsible for maintaining the confidentiality of its account and password and for restricting access to their computers and other internet platforms. User will agree to accept responsibility for all activities that occur under its account and/or password. If any unauthorized person obtains access to bugle SaaS Service as a result of any act or omission by the user, he/she shall use its best efforts to ascertain the source and manner of acquisition and shall fully and promptly brief bugle. User shall otherwise cooperate and assist in any investigation relating to any such unauthorized access.

2. Security Measures

2.1 Access control to premises and facilities

Measures are in place to prevent unauthorized physical access to premises and facilities holding personal data.

2.2 Access control to systems

Measures are in place to prevent unauthorized access to IT systems.

2.3 Access control to data

Measures are in place to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data.

2.4 Disclosure control

Measures are in place to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged.

2.5 Input control

Measures are in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

2.6 Job control

Measures are in place to ensure that data is processed strictly in compliance with the data importer's instructions.

2.7 Availability control

Measures are in place to ensure that data is protected against accidental destruction or loss.

2.8 Segregation control

Measures are in place to allow data collected for different purposes to be processed separately.

2.9 Disaster Recovery Plan

Measures are in place to ensure the key elements of a Disaster Recovery Plan. If data, IT systems and networks are disrupted, this plan will assure there are processes in place to certify that the business can be recovered in an emergency.

2.10 Business Continuity Plan

Measures are in place for the key elements of a Business Continuity Plan. The function of the Business Continuity Plan is to assist impacted areas in ensuring that critical business functions are maintained, restored, or augmented to meet the designated Recovery Time and recovery strategies outlined in the areas' business continuity and business resumption plans.

3. Network Security

bugle has measures in place to prevent eavesdropping between the customer and customers' users and bugle systems, as well as within bugle infrastructure. All network traffic runs over SSL/HTTPS. Internal infrastructure is isolated using strict firewalls and network access lists. Each system is designated to a firewall security group by its function. By default, all access is denied and only explicitly allowed ports are exposed. Persistence and storage layers are encrypted and secured behind VPN & VPC firewalls.