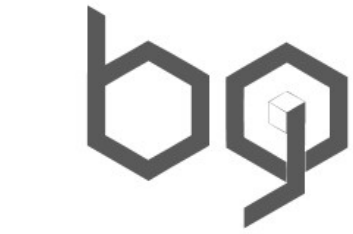
http://www.weekly10.net/terms/privacy



binary geek limited

BGL-PL-102

Weekly10 General Privacy Policy

Updated 2nd May 2018

Contents

Overview

Last Update	**16 April 2018**
Effective Date	2nd May 2018

We are committed to safeguarding the privacy of our website visitors and application users; in this policy we explain how we will treat Personal Data. By agreeing to this policy, you consent to your responsibilities outlined in this document.

1.0 Purpose & Scope

This policy sets out how BGL seeks to protect Personal Data and ensure that our staff understand the rules governing their use of the Personal Data to which they have access during their work. This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. For the purposes of this policy the use of the term 'website and platform' refers to both http://www.weekly10.net (marketing website) and https://app.weekly10.net (the application). This policy may reference other official policies denoted by BGL-PL-XXX. These policies are available on request; however certain policies may be subject to a signed Non-Disclosure Agreement (NDA).

As our data protection officer (DPO), Andrew Roberts has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Email: andrew.roberts@weekly10.net

2.0 Definitions

Amazon Web Services (AWS)	We use AWS to provide our website and Software as a Service (SaaS) platform. Thus, AWS acts as a Data Processor as set out in this policy and the accompanying signed Data Processing Addendum (DPA)
Content	Data uploaded to or entered into our website or platform which is not related to account or customer meta-data (such as email address and name). This includes employee goals, questions and feedback.
Data Controller	'Data 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; where the purposes and means of such processing are determined by law.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.
Data Subject	a natural person whose Personal Data is processed by a controller or processor
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 or an online identifier.

Processing	'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.
Privacy by Design	An approach to our website and platform that promotes privacy and data protection compliance from the start. This is implemented through a variety of TOMs as highlighted within this policy.
Special categories of Personal Data (or Sensitive Personal Data)	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information.
Technical & Organisational Measures (TOMs)	Technical measures which we have taken and organisational processes which we have implemented to ensure compliance to this policy.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office (ICO).
User Data	The Personal Data listed at paragraph 3.1.

3.0 Data Protection Roles & Responsibilities

BGL minimises the control and processing of Personal Data to the lowest necessary level. We only act as Data Controller for data required for the administration of customer accounts. For all remaining data stored and processed on our website and platform we and our cloud hosting partner (AWS) act as a Data Processor.

3.1 BGL and you are a joint Data Controller for the following User Data:

(a) A users' full name

(b) Email address

(c) Mobile phone number

(d) Business address

(e) Profile images

3.2 You, as a customer are a Data Controller for the following Personal Data:

(a) Any data 'content' inputted into the website or platform that contains Personal Data other than that referenced in 3.1, which includes but is not limited to employee goals, questions, feedback and uploaded attachments

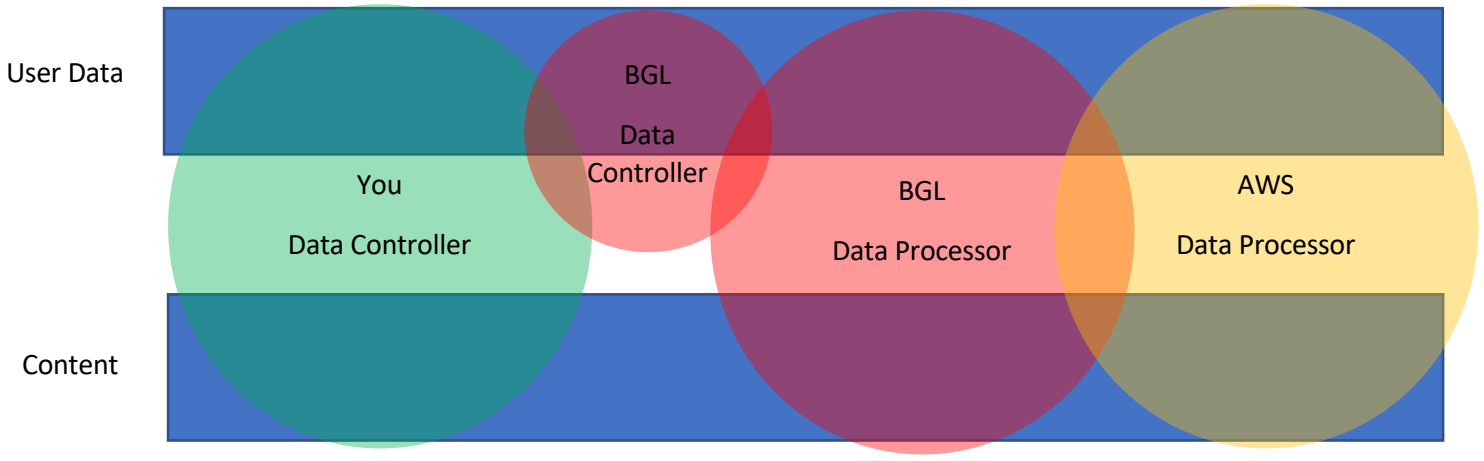
(b) Any data which is derived or generated from the analysis or reporting of Personal Data originating from either 3.2(a) or 3.1

3.3 BGL is a Data Processor for

(a) All data on the platform including data referenced in 3.1 and 3.2

3.4 AWS acts as a Data Processor as an authorised 3rd party to BGL for

(a) All data on the platform including data referenced in 3.1 and 3.2



4.0 Processing Anonymous Information

4.1 We use Google Analytics (GA) to monitor and optimize the performance of our website and platform. We have a signed DPA in place with Google to in relation to data processing. We send no Personal Data to GA. Using GA, BGL may collect, store and use the following kinds of anonymous information:

(a) Information about your computer and about your visits to and use of this website (including your geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths);

(b) Information contained in or relating to any communication that you send to us or send through our website or email (including the communication content and metadata associated with the communication);

5.0 Consent

5.1 We obtain a Data Subject's consent when a user either signs up to our website and platform or when we make modifications to this policy via our platform. We store a record of this consent for the control and processing of data set out in 3.1

5.2 You, as Data Controller, must obtain and record a Data Subject's consent before recording their Personal Data as content within our website or platform.

5.3 We obtain and record consent from our website and platform users to collect anonymous information including the use of cookies. This consent is obtained when visiting our website or when verifying a new user account.

6.0 Using Personal Data

6.1 BGL may use Personal Data outlined in 3.1 to:

(a) administer the service we provide via our website and platform

(b) personalise our website and platform for you;

(c) enable your use of the services available on our website;

(e) supply to you services purchased through our website or as part of a contract

(f) send statements, invoices and payment reminders to you, and collect payments from you;

(g) send you non-marketing commercial communications;

(h) send you email notifications that you have specifically requested;

(i) send you our email newsletter, if you have requested it (you can inform us at any time if you no longer require the newsletter);

(j) send you marketing communications relating to our business which we think may be of interest to you, by post or, where you have specifically agreed to this, by email or similar technology (you can inform us at any time if you no longer require marketing communications);

(k) provide third parties with statistical information about our users (but those third parties will not be able to identify any individual user from that information);

(l) deal with enquiries and complaints made by or about you relating to our platform or website;

(m) keep our website secure and prevent fraud; and

(n) verify compliance with the terms and conditions governing the use of our website.

7.0 Disclosing Personal Data

7.1 BGL may disclose Personal Data from clause 3.1 where required to any of our employees or subcontractors insofar as reasonably necessary for the purposes set out in this policy.

7.2 BGL will not, without your express consent, supply Personal Data to any third party for the any purpose other than outlined in 7.1

7.3 BGL may disclose your Personal Data:

(a) in connection with any ongoing or prospective legal proceedings where requested by a relevant authority;

(b) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);

(c) to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that Personal Data where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that Personal Data.

7.4 Except as provided in this policy, we will not provide your Personal Data to third parties.

7.5 We will not disclose or control any content from clause 3.2 which you enter or upload to our website or platform to 3rd parties except as necessary to comply with law or a court order.

8.0 Data Transfers

8.1 Information that we collect may be stored, processed and transferred only within the European Economic Area (as of January 2018).

9.0 Retaining Personal Data

This Section 9 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of Personal Data.

9.1 Personal Data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

9.2 Without prejudice to 9.1, we will delete Personal Data falling within the categories set out below at the date/time set out below:

(a) User data (i.e. email, profile information) outlined in 3.1 will be deleted 60 days after an account has been closed.

(b) All content (i.e. Goals and questions) outlined in 3.2 which may contain Personal Data will be deleted 60 days after an account has been closed. We will retain report data for a maximum of 5 years for an active account.

(c) All attachment data outlined in 3.2 which may contain Personal Data will be deleted 60 days after an account has been closed. We will retain attachment data for a maximum of 5 years for an active account.

9.3 Notwithstanding the other provisions of this Section 9, we will retain documents (including electronic documents) containing Personal Data:

(a) to the extent that we are required to do so by law;

(b) if we believe that the documents may be relevant to any ongoing or prospective legal proceedings; and

(c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

10.0 Security of Personal Data

10.1 We will take reasonable technical and organisational measures (TOMs) to prevent the loss, misuse or alteration of your Personal Data.

10.2 We will store all the Personal Data you provide on secure (multi-factor authenticated- and firewall-protected) servers. Personal Data is encrypted at rest on our database using AES-256 encryption and when sent over internal and external networks (via HTTPS). Our Server Security Policy BGL-PL-103

10.3 All electronic financial transactions entered into through are handled by a third party payment provider. We do not store any payment details on our servers.

10.4 You are responsible for keeping the password you use for accessing our website confidential; we will not ask you for your password (except when you log in to our website or platform)

10.5 As a Data Controller for profile information our employees or sub-contractors may have access to this information only for the purposes of providing support or in the operation of the platform

10.6 As a Data Processor for your content our employees or sub-contractors do not have un-encrypted access to your content

10.7 Both Personal Data and content is backed up regularly (no less than every hour) and tested in-line with our Business Continuity Plan (BCP) BGL-PL-104. All back-ups are stored in an encrypted state.

11.0 Data Breach Identification & Notifications

11.1 We continuously test and validate our website and platform for vulnerabilities using a variety of means including penetration testing, ethical hacking, cross-site scripting testing and security scanning.

11.2 We continuously monitor our infrastructure, website and platform for threats and attacks using a variety of means including tools provided to us by our cloud infrastructure partner AWS.

11.3 We will notify the ICO as soon as feasibly possible but within 24 hours of a data breech. Where our 3rd party infrastructure provider (AWS) reports a data breach relating to our platform we will notify the ICO immediately upon receipt of information.

11.4 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

(a) Investigate the failure and take remedial steps if necessary

(b) Maintain a register of compliance failures

(c) Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

(d) Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

11.5 The full procedure for how we identify and handle a Data Breach is detailed in our Information Security Incident Procedure BGL-PL-107.

12.0 Your Rights

12.1 BGL endeavor to make all Personal Data for which we are Data Controller available to our users via their personal platform account. However, a Data Subject may instruct us to provide you with any Personal Data we hold about you via a Subject Access Request; We will provide this service free of charge within 28 days of request under the following conditions:

(a) The individual supplies appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address)

(b) For unfounded or excessive, or repetitive requests we reserve the right to charge a reasonable fee to cover administration costs

12.2 BGL may withhold Personal Data if required to do so by law.

12.3 A Data Subject may instruct us at any time not to process or delete their Personal Data. In doing so they may not be able to use our services. We will do this within 28 days of request under the following conditions:

(a) The individual supplies appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address)

12.4 A Data Subject will expressly agree in advance if we are to use their Personal Data for marketing purposes.

13.0 Key Technical & Organisational Measures (TOMs)

We have implemented a range of TOMs to ensure that we adopt a Privacy by Design approach to the development and operation of our website and platform. Several key measures are highlighted below:

13.1 Our staff and sub-contractors have no access to your 'content'. Data is encrypted and is not available from our support or operational accounts or dashboards. We only act as a 'Data Processor' for this data

13.2 All data where we act as a 'Data Controller' is prohibited from being printed and is only viewable on secure internally viewable dashboards to relevant employees

13.3 All data is encrypted at rest using AES-256 encryption algorithms. When back-ups are made, these are stored in an encrypted state

13.4 All data in transit over a network both internally and externally (internet) is encrypted using SSL or TLS technologies

13.5 Our platform runs entirely on AWS. We have an agreed DPA in place with AWS which is ensures AWS operates under GDPR standards and regulations.

13.6 We implement a strict Server Security Policy BGL-PL-103 which limits access to our production environment to only those employees or sub-contractors that have a declared reason for access

13.7 We have a well-defined Information Security Incident Procedure BGL-PL-107 which details how we handle a Data Breach on our platform as both a 'Data Controller' and 'Data Processor'

13.8 Our platform is built on modern up to date and well maintained technology with inherently secure data processing. We maintain security updates an and automated update process handled by AWS.

14.0 General Staff Guidelines

14.1 The only people able to access data covered by this policy are those who need it for their work.

14.2 Data is not shared informally. When access to confidential information is required, employees can request it from their line managers.

14.3 BGL provides training to all employees to help them understand their responsibilities when handling data.

14.4 Employees keep all data secure, by taking sensible precautions and following the guidelines of our Server Security Policy BGL-PL-103

14.5 Personal Data should is not be disclosed to unauthorised people, either within the company or externally.

14.6 Content is not viewable by BGL staff members or sub-contractors unless explicitly approved by the respective customer.

15.0 Third Party Websites

15.1 Our website or platform may include hyperlinks to, and details of, third party websites.

15.2 We have no control over, and are not responsible for, the privacy policies and practices of third parties.

16.0 Updating Information

16.1 If a Data Subject believes Personal Data we hold as a Data Controller is incorrect, they may notify us at contact@weekly10.net and we will update this information as soon as possible (at most within 7 days of notification).

17.0 Cookies

17.1 Our website and platform uses cookies.

17.2 A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

17.3 Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

17.4 Cookies do not typically contain any information that personally identifies a user, but Personal Data that we store about you may be linked to the information stored in and obtained from cookies.

17.5 We both session and persistent cookies on our website.

17.6 The names of the cookies that we use on our website, and the purposes for which they are used, are set out below:

(a) We use _utma (unique visitor cookie), _utmb (session cookie) and _utmc (session cookie) to analyse your movement through our website and improve the overall user experience.

17.7 Most browsers allow you to refuse to accept cookies; for example:

(a) in Internet Explorer (version 11) you can block cookies using the cookie handling override settings available by clicking "Tools", "Internet Options", "Privacy" and then "Advanced";

(b) in Firefox (version 47) you can block all cookies by clicking "Tools", "Options", "Privacy", selecting "Use custom settings for history" from the drop-down menu, and unticking "Accept cookies from sites"; and

(c) in Chrome (version 52), you can block all cookies by accessing the "Customise and control" menu, and clicking "Settings", "Show advanced settings" and "Content

settings", and then selecting "Block sites from setting any data" under the "Cookies" heading.

17.8 Blocking all cookies will have a negative impact upon the usability of many websites.

17.9 If you block cookies, you will not be able to use all the features on our website.

17.10 You can delete cookies already stored on your computer; for example:

(a) in Internet Explorer (version 11), you must manually delete cookie files (you can find instructions for doing so at http://windows.microsoft.com/en-gb/internet-explorer/delete-manage-cookies#ie=ie-11);

(b) in Firefox (version 47), you can delete cookies by clicking "Tools", "Options" and "Privacy", then selecting "Use custom settings for history" from the drop-down menu, clicking "Show Cookies", and then clicking "Remove All Cookies"; and

(c) in Chrome (version 52), you can delete all cookies by accessing the "Customise and control" menu, and clicking "Settings", "Show advanced settings" and "Clear browsing data", and then selecting "Cookies and other site and plug-in data" before clicking "Clear browsing data".

17.11 Deleting cookies will have a negative impact on the usability of many websites.

18.0 Audits, monitoring and training

18.1 This policy will be reviewed every 12 months, or sooner in-line with any changes in data protection legislation or Personal Data collection, control and processing

18.2 This policy will be audited every 12 months during our BCP testing cycle as detailed in our Business Continuity Plan (BCP) BGL-PL-104.

18.3 BGL provides training to all employees to help them understand their responsibilities when handling data in-line with the latest legislation. Employees and sub-contractors are required to participate in ICO online training at least once every 12 months

19.0 Amendments

19.1 BGL may update this policy from time to time by publishing a new version on our website.

19.2 We will notify you of changes to this policy by email and/or through our platform.

14.0 Data Protection Registration

14.1 We are registered as a Data Controller with the UK Information Commissioner's Office.

14.2 You can view our data protection registration at https://ico.org.uk

15.0 Our Details

15.1 This website and platform is owned and operated by Binary Geek Limited.

15.2 We are registered in England and Wales under registration number 08225904

15.3 You can contact us:

(a) by email, using the email address published on our website from time to time.

16.0 Related Standards, Policies and Plans

- BGL-PL-101_IT_Equipment_and_Applications_Security_Policy
- BGL-PL-103_Server_Security_Policy
- BGL-PL-104_Business_Cotinuity_Plan
- BGL-PL-107_Information_Security_Incident_Procedure
- AWS_Data_Processing_Addendum_DPA_2016-12-12