ITJobs.tech GDPR Commitment & FAQ

Introduction

This document aims to help IT Consulting Piotr Wozniak's ITJobs.tech customers with common questions that arise in the context of the EU General Data Protection Regulation (GDPR).

Our Commitment

ITJobs.tech will comply with applicable GDPR regulations as a data processor when they take effect on the 25th of May 2018. Working together with our customers, we will explore opportunities to develop the ITJobs.tech platform to assist our customers to meet their GDPR obligations.

Frequently asked questions

What categories of personal data do you process on our behalf?

Categories of Individuals	Categories of Personal Data
Job seekers	Contact details (name, email, address, etc)
	Professional history (employment history, education, skills, etc)
	CV documents
	Application history
	Job search/alerts preferences
	Email marketing preference
Recruiter users	Contact details (name, email, phone, etc)
Contact us form submitters Contact details	Contact details
Website visitors	IP addresses, usage data
CMS users	Contact details
	IP addresses, usage data

Please note that the product supports custom application screening questions which may not be covered by the above.

Do you process any sensitive/special category data on our behalf?

No*, it is our understanding that none of the above categories of personal data fall under the GDPR's definition of Special category of data.

* except if you have custom application screening questions that fall under the scope of special category data.

What steps are your taking to ensure your data processing complies with the GDPR?

We have concluded a GDPR readiness project to confirm that applicable GDPR provisions are covered off by our internal company policies & procedures, and have confirmed our compliance with applicable GDPR provisions, and internal company policies & procedures.

What are your GDPR related contract terms?

Our service contract terms include provisions for the following compulsory contract details/terms:

1. the subject matter and duration of the processing;
2. the nature and purpose of the processing;

3. the type of personal data and categories of data subject; and
4. the obligations and rights of the controller
5. the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
6. the processor must ensure that people processing the data are subject to a duty of confidence;
7. the processor must take appropriate measures to ensure the security of processing;
8. the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
9. the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
10. the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
11. the processor must delete or return all personal data to the controller as requested at the end of the contract; and
12. the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

(source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/)

JobBoard.com's Terms & Conditions can be found here:

www.itjobs.tech/terms

What are your technical & organisational measures for ensuring the security of processing?

In broad terms our technical & organisational measures include:

1. Training
2. Written policies and procedures
3. Access controls
4. Encryption
5. Backups
6. Audits

In more detailed terms, our organisational measures include:

1. Staff are regularly trained on data protection & data privacy
2. Staff are bound by a confidentiality clause
3. There is a dedicated information security group with staff dedicated to maintaining the organisations information security posture
4. Staff with an information security responsibility undergo additional security related training
5. Access to your data by our staff is access controlled, and access is granted & reviewed strictly in accordance with need-to-know/least-privilege principles
6. PCI DSS compliance is on record
7. Vulnerability tests are completed quarterly and attested
8. Pen tests are completed yearly by a third party company
9. Web applications follow security guidelines (OWASP)
10. There is an established process for performing due diligence and vetting new service providers. A risk assessment is performed on third parties that includes:
    a. A controls assessment that includes a process for issue tracking and remediation.
    b. Confidentiality and/or non-disclosure agreements are in place for all third parties.
11. There is a continual service improvement program in place
12. We have the following organisational policies in place with provisions relevant to GDPR: (Policies are reviewed at a minimum every 12 months.)
    a. Information Security Policy
    b. Remote Access Policy
    c. Virtual Private Network Policy
    d. Mobile Device Security Policy
    e. Mobile and Storage Device Policy
    f. Password Policy
    g. Business continuity
    h. Acceptable use of company assets and resources (computers, information, etc.)
    i. Access control
    j. Desktop computing
    k. Disaster recovery
    l. Personnel security and termination
    m. Physical access
    n. Policy maintenance
    o. Security incident event/response management

p. Secure disposal of hardware and assets
q. Vulnerability management
r. Asset management
s. Change management

In more detailed terms, our technical measures include:

1. Access controls:
    a. Network access control (Firewalls, IP range restrictions, VPNs)
    b. Username/password access control
    c. 512 bit access key based access control
2. Regular software updates
3. Real-time protection anti-virus, anti-malware and anti-spyware software
4. Data at Rest encryption
5. Data in Transit encryption*
6. Secure password hashing
7. Data backups

(* We use Data in Transit encryption for all transmissions where we control both ends of the transmission. We do not control your, or your job seekers' mail servers, if these do not support Data in Transit encryption then personal data may be transmitted in 'plain text'. Furthermore, we highly recommend you purchase an SSL certificate for use with your JobBoard.com website, if you choose not to do so, then personal data may be transmitted in 'plain text'.)

ITJobs.tech is hosted on Microsoft Azure's cloud platform. Azure meets a broad set of compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. (source: https://azure.microsoft.com/en-en/overview/trusted-cloud/)

Where is the personal data located? How is it stored? Is it separate from your other customers' data?

Your data is hosted in the EU. It's stored in a SQL database, and blob storage. All your data is kept separate from our other customers.

Do you transfer personal data to non-EU countries or international organisations?

We do not transfer personal data to 'international organisations' as defined by GDPR (UN, NATO, etc.).

Your data is hosted in the EU, and we do not transfer it out of the EU, except:

1. Scenarios outside of our control:
    a. If a job seeker accesses their account from a non-EU country
    b. If you access the ITJobs.tech CMS from a non-EU country
    c. If your customers (recruiters/advertisers/employers) access their Recruiter Account area from a non-EU country
    d. If you have configured email notifications to be send to recipients outside the EU, or which are processed by mail servers outside the EU
    e. If your customers (recruiters/advertisers/employers) have configured email notifications (e.g. Application email notification) to be send to recipients outside the EU, or which are processed by mail servers outside the EU
2. Microsoft Azure Support:
    a. Your data is hosted in Microsoft Azure's EU data centers. We may occasionally ask Microsoft Azure Support to help us diagnose an issue, this may involve granting tchem access to your database. In this eventuality, a Microsoft Azure Support engineer outside of the EU may access your data.
    b. Microsoft are EU-US Privacy Shield certified: https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK
    c. Microsoft offers EU Standard Contractual Clauses, guarantees for transfers of personal data: https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses
    d. Further information: https://www.microsoft.com/en-us/trustcenter/privacy/who-canaccess-your-data-and-on-what-terms
        i. Access to data by Microsoft employees is subject to various access controls and auditing
        ii. Microsoft's Sub-processors are subject to the same controls as Microsoft employees
        iii. Microsoft's Sub-processors are required to meet GDPR requirements
        iv. Microsoft's Sub-processors must agree to the EU Model Clauses for services for which Microsoft offers

Lastly, we use a Sub Processor (Google Analytics) to provide us with anonymised site & CMS usage data analytics. Our data processing agreement with Google covers all the required GDPR provisions. Google

are EU-US Privacy Shield certified: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI

Do you have a Data Protection Officer?

Yes.

What product features can help us with our GDPR compliance?

The following features have been developed in cooperation with our customers to help with your compliance:

1. You can upload a cookie notice introductory message, and a privacy policy page via the CMS
2. A compulsory accept terms of use/privacy policy tick box can be added upon request to the following forms:

   * if you wish this feature to be activated please contact your account manager and let us know the wording for the tick box.

   a. Registration & application forms
   b. Contact us form
   c. Blog comment form
3. A compulsory form can be added upon request to your site to be presented after a job seeker logs into their account showing the optional newsletter opt in consent tick box (if enabled), compulsory point 4 consent tick box (if enabled), and compulsory point 5 registration form terms of use tick box (if enabled). When a job seeker logs in that registered or last logged in prior to a configurable date the job seeker will be required to submit the form before they can access My Account area features (access to Close My Account form will still be permitted)
4. To allow evidencing of consent, a record will be kept indefinitely with the following information each time a form containing one or more of the following tick boxes is submitted: newsletter opt in consent tick box, cv search consent setting, point 2 terms of use/privacy policy tick box:

   a. Date/Time
   b. Candidate GDPR Evidence Ref (if registering or logged in at time of submission)
   c. Name
   d. Email
   e. URL of form (e.g. www.site.co.uk/candidate/register/)
   f. Given/withdrawn

g. Text of tick box

5. You control the areas in the ITJobs.tech CMS that your staff have access to. This allows you to control access to those areas dealing with personal data in accordance with need-to-know/leastprivilege principles.
6. Excel reports/exports that include personal data are encrypted with a compulsory password
7. Google Analytics IP address anonymization can be enabled upon request
8. 'Soft' deleted CVs, Candidates, and Job Alerts are automatically 'hard' deleted 14 days later (enabled by default; can be disabled upon request)
9. Inactive job seeker profile/CVs retention policy can be enabled upon request
10. Application retention policy can be enabled upon request
11. Application expiry for recruiters (to hide old applications from their online account area) can be enabled upon request

What 'cookies' does our ITJobs.tech website use?

In the standard configuration ITJobs.tech website may use the following cookies.

Cookie Name	**Purpose / Description**	**Expiration Time**
cookienoticecookie	Saves information to allow the website to determine whether or not to display a visitor the cookie notice. Contains the version of the cookie notice last displayed, the number of times it has been displayed, and whether it has been acknowledged.	180 days
ASP.NET_SessionId	Stores a unique session identifier upon accessing the first page in a session, and allows functions to access information submitted earlier in the session. The following functions use this cookie: Login with Facebook/LinkedIn - Essential to allow the site to return the user back to the correct page after returning from Facebook/LinkedIn's login form.	When visitor closes their browser

	Shortlisted jobs - Essential to keep track of which jobs a non-logged in user has shortlisted. Job alert activity report - Essential to be able to count the # Responses (apps/clicks) originated from job alert emails. Blog comment form - Essential to be able to display the submitted comment after the comment has been posted. Most recent job search result page sign posting - Essential to be able to link back to the most recently view job search results page. Poll submission form - Essential to ensure only one vote is counted per user. Post a job with recruiter registration/check out flow - Essential to remember the job details during the multi page registration & checkout flow Most recent candidate search results page sign posting - Essential to be able link back to the most recently viewed candidate search page.	
ASPXAUTH	Stores an encrypted identifier of the job seeker upon successful login. Essential to ensure that a job seeker only has to login once per session.	When visitor closes their browser, or when the user logs out

Google Analytics cookies		
_ga	Used to distinguish users (to help count how many people visit your site by tracking if you've visited before)	2 years
_gid	Used to distinguish users (to help count how many people visit your site by tracking if you've visited before)	24 hours
_gat_customerTracker	Used to throttle request rate.	1 minute
_gat	Used to throttle request rate.	1 minute
We use Google Analytics for anonymised site usage analysis to help us improve JobBoard.com, therefore your site will always use Google Analytics even if you do not configure it explicitly for your own purposes. Other Google Analytics cookies may depending on configuration also be set, see https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage		

With respect to 'minimally intrusive' cookies (e.g. Google Analytics) a UK government source has this to say:

The ICO guidance supports this view as it states "...it is highly unlikely that priority for any formal action would be given to focusing on uses of cookies where there is a low level of intrusiveness and risk of harm to individuals. Provided clear information is given about their activities we are unlikely to prioritise first-party cookies used only for analytical purposes in any consideration of regulatory action" (source: https://gds.blog.gov.uk/wp-content/uploads/sites/60/2012/03/gds-cookiesimplementer-guide.pdf).

In January 2017, the European Commission clarified the high-level privacy rules as follows:

The so called "cookie provision", which has resulted in an overload of consent requests for internet users, will be streamlined. New rules will allow users to be more in control of their settings, providing an easy way to accept or refuse the tracking of cookies and other identifiers in case of privacy risks. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history). Cookies set by a visited website counting the

number of visitors to that website will no longer require consent." (source: http://europa.eu/rapid/press-release_IP-17-16_en.htm).

All of the cookies above are 'first-party' cookies. Furthermore these cookies are either 'minimally intrusive', or exempt from regulations altogether, in other words, **the above cookies do not require consent.**

What's your policy for dealing with the various Data Subject rights?

Data Subjects (e.g. Job seekers) have the following rights:

1. Right to be informed
2. Right of access
3. Right to rectification
4. Right to erasure
5. Right to restrict processing
6. Right to data portability
7. Right to object

What's your policy for personal data breach notification?

We will inform you without undue delay as soon as we become aware of a data breach. We will assist you in meeting your GDPR breach obligations, including:

1. Article 33 - Obligation to notify personal data breaches to your supervisory authority (e.g. ICO in the UK)
2. Article 34 - Obligation to advise data subjects when there has been a personal data breach

We have prepared a response plan for addressing any personal data breaches that occur, and have allocated responsibility to our Data Protection Officer for managing data breaches.

If you are GDPR compliant, does that mean I'm GDPR compliant?

We comply with applicable GDPR regulations as a data processor, and we are confident ITJobs.tech offering can be used in a compliant manner. However, it doesn't automatically follow that your use of our product, and/or your overall business is GDPR compliant. You will need to take your own legal advice.

I'm still confused/worried…

You're not alone. We observe that the headline grabbing fines have induced a degree of mass hysteria, we believe this to be misplaced. It's important to keep a healthy perspective, and we leave you with a couple of quotes:

1. "The legislation is four to five times more complicated than existing law. We'll probably spend the next 20 years figuring out what it means to be compliant," Eduardo Ustaran of Hogan Lovells, a law firm.
2. "We're not going to be looking at perfection, we're going to be looking for commitment," Elizabeth Denham, head of the Information Commission Office.