

Recruitment Candidate Privacy Notice (EU)

Last update: 16 March 2018



Scope and Aims

This Privacy Notice ("Notice") explains how Dentsu Aegis Network collects and uses candidate personal information within the European Union (EU) and how that information is kept secure.

Please note that there may be additional guidance issued in the country that you are employed in. Wherever such local guidance may be required to enable compliance with any local law or regulation, if that local guidance is in any respect inconsistent with this document, this document shall only apply to the extent that it is consistent, or may be made consistent, with that local guidance from time to time.

For current employees, the separate EU Employee Privacy Notice will cover internal recruitment activities.

Your Information and Privacy

At DAN, we take privacy very seriously. We do need your information so that we can provide world class recruitment services to you, however protecting your information and respecting your privacy is fundamental to maintaining your trust. Our Global Privacy Principles can be found [here](#)

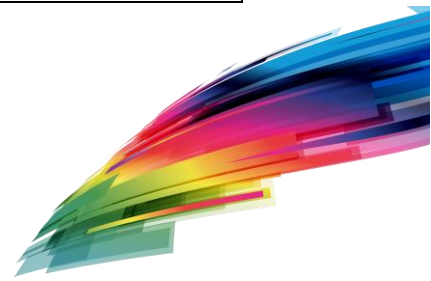
This Privacy Notice refers to certain legal words or phrases. You can spot them easily: they're displayed in a [different colour](#) the first time they're used. In case you're unsure what these words and phrases mean, we've provided some [definitions](#) at the end of this Privacy Notice.

Dentsu Aegis Network and its group of organisations ("DAN", "we", "our" or "us") utilise global HR information systems ("HRIS") for recruitment purposes and to capture and store personal data on potential employees and recruitment candidates.

What type of personal data do we collect about you as part of the recruitment process?

We collect and use different types of personal information about you, depending on your circumstances, your role and the law. This list below is illustrative and non-exhaustive.

Type of Information	Examples
Information to contact you at work or home	name, address, telephone, and e-mail addresses.
Information about who to contact in a case of emergency (yours or ours)	name, address, telephone, e-mail addresses and their relationship to you.
Information to identify you	Photographs, passport and/or driving licence details, electronic signatures, national insurance or social security numbers (where applicable).
Information about your suitability to work for us and/or a relevant third party:	References, interview notes, work visas, ID information such as passport details and driving licence information, records/results of pre-employment checks, including criminal record checks, credit and fraud checks.
Information about your skills and experience	CVs, resumes and/or application forms, references, records of qualifications, skills, training and other compliance requirements.
Additional data that we may request where permitted by law.	We may, subject to local laws, ask you to register your personal profile which could include declaring information about your ethnicity, disability, age, religion/belief, gender and sexual orientation.



Who collects your personal data?

Your personal data is collected by the [DAN organisation](#) for purposes of the recruitment process, where, if successful, you may enter into an employment contract. This DAN organisation is a [data controller](#) in relation to the personal data that's collected about you.

How is your personal data collected?

We collect personal data from you and from other organisations, as described below.

You provide personal data about yourself and others

This is personal data that you provide to the local HR Recruitment team or enter directly into DAN recruitment systems (where applicable).

You may also provide us with personal data about others, notably your dependents and other family members. This tends to happen for HR administration and management reasons, eg emergency contact details.

We may collect personal data from other organisations

We may obtain information about you from other organisations. For example, we may gather references from your previous employer(s); medical reports from external professionals; and, the results of a background check (where permitted by applicable law).

How do we use your personal data?

We may collect and further process your personal data for various purposes subject to local law and any applicable collective bargaining agreements. Please note, that the list below is not an exhaustive list of the purposes for which we process personal data for recruitment purposes.

Purposes for which we need your personal information:	Examples
Recruitment	To assess your suitability to work for DAN; <ul style="list-style-type: none"> To perform requisition and applicant management activities; To perform precision matching to job vacancies; To conduct screening, assessments and interviews; To maintain a library of correspondence; To make offers and provide contracts of employment; To conduct pre-employment checks, including determining your legal right to work and carrying out criminal record and credit checks where applicable
To operate the relationships with customers and suppliers	This may include <ul style="list-style-type: none"> the disclosure to customers of relevant vetting information (in line with the appropriate requirements of regulated customers), contact details, curriculum vitae information, or photographic images.
Fraud prevention	We may check your details with/against fraud prevention databases
Diversity Information	In some countries we may, subject to local laws, ask you to register with us your personal profile which could include declaring information about your ethnicity, disability, age, religion/belief, gender and sexual orientation. This information is used to help us improve our employment practices and access to this information is strictly limited.

Additional information about the ways in which DAN processes your personal data may be notified to you locally.



What are our legal bases for processing your personal data?

Data protection laws may require that we only process your personal data where we have a legal basis for doing so. In compliance with these laws, our processing activities are done on one or more of the following legal bases:

- The processing is necessary for our compliance with a legal obligation;
- The processing is necessary for legitimate interests that are pursued by us or by a third party.
- The processing is necessary for the performance of a contract to which you are party, or in order to take steps at your request prior to you and the DAN organisation entering into such a contract.

Processing of sensitive personal data

Our processing of sensitive personal data is done on one or more of the following legal bases. The processing is necessary:

- For the purposes of carrying out our/your obligations or to exercise our/your specific rights under employment, social security or social protection law, to the extent permissible under applicable laws;
- to protect your vital interests or the vital interests of another person where you or they, as applicable, are physically or legally incapable of giving consent (for example in a medical emergency);
- for the establishment, exercise or defence of legal claims
- solely to the extent that our processing of your sensitive personal data cannot be justified by one or more of the legal bases described above, we will obtain your consent to our processing of that personal data. This consent will be obtained from you separately.

Where we have sought your consent to the processing of your sensitive personal data, you may withdraw this consent by contacting your local HR recruitment team. Where you have withdrawn your consent but we retain the sensitive personal data, we will only process that data where we have another legal basis on which to do so (for example, where we need to process your personal data in order to carry out our obligations under employment law). You should note that the withdrawal of consent may prevent us from carrying out certain tasks. For example, contacting your next-of-kin in an emergency.

Processing of Personal Data Relating to Criminal Convictions and Offences

Personal data relating to criminal convictions and offences will only be processed by DAN where authorised to do so by applicable law. For example, a criminal record check may be carried out on recruitment where authorised by law

Who has access to your personal data?

We may share your personal information between DAN organisations and use it for the purposes set out in this privacy notice. We may need to grant organisations outside of DAN access to your personal data. We will always take appropriate measures to keep your personal information confidential, secure and protected, including when we need to share it with our trusted partners.

Dentsu Aegis Network uses all reasonable means to ensure that third party sources use your personal information only for the purposes for which it was provided and in adherence to the Dentsu Aegis Network Privacy Policy.

Is your personal data sent to other territories?

Your personal data may be shared with other DAN organisations as well as organisations outside of DAN.

We may transfer your personal information to other countries (and may store it there), where our people (or suppliers) may process it. When this happens, we'll make sure we follow the requirements of the law and that your personal information is always protected by the same security standards we follow.

How long do we keep your personal data?

We only hold your personal data for as long as there is a business need or a legal obligation to keep it.

Your rights

You have a number of rights in respect of your personal data. We've detailed these rights below.

Accessing your personal data

You have the right to request a copy of the personal data that DAN holds about you.

Keeping your personal data correct and up-to-date

You have a right to request that any inaccuracies in your personal data are corrected. It is important that the personal information we hold about you is kept accurate and up to date. We therefore need you to inform us of any change or update to your personal information.

Deleting and blocking use of personal data

You have the right to request the deletion or blocking of any irrelevant personal data we hold about you, or you may be entitled to object to our continued processing of your personal data.

Where you have been asked to provide your consent to our processing of your personal data, please note that you may withdraw such consent at any time by contacting your local HR Recruitment Team.

You should note that the withdrawal of consent may prevent us from carrying out certain tasks within the recruitment process.

Other rights if you are in France

If you are in France, you also have the right to issue general or specific directives regarding the disposition of your personal data after your death.

If you are an EU Citizen, there are additional rights available (from 25 May 2018)

From 25 May 2018, you also have the following rights:

- *Data portability* – You may request that we provide you with the personal data that we hold on file about you and, where technically feasible, to transmit such data to another organisation – there are limitations to this under law
- *Right to restriction of processing* - There are certain situations where you can restrict our processing of your personal data
- *Right to withdraw consent* – Where we are relying upon your consent to process personal data, you have the right to withdraw such consent at any time.
- *Right to object to processing justified on legitimate interest grounds* - Where your personal data is processed because of a legitimate interest purpose, you have the right to object to such processing.
- *Right to be forgotten* – You have the right to request that we erase your personal data where:
 - the personal data is no longer necessary for the purposes it was originally collected;



- our processing of your personal data is based solely upon your consent, and you withdraw your consent;
- we are relying on the legal basis of legitimate interests to process your personal data (unless we can demonstrate compelling legitimate grounds for our processing of your personal data and those grounds override your interests); or
- your personal data has been unlawfully processed, or must be erased for compliance with an applicable legal obligation under EU or an EU member state's law.

In addition to the rights stated above, you have the right to lodge a complaint with a supervisory authority.

How do we keep your personal data safe?

We have security arrangements in place to guard against unauthorised access, improper use, alteration, destruction or accidental loss of your personal information.

We take appropriate organisational and technical security measures and have rules and procedures in place to ensure that any personal information we hold on computer systems is not accessed by anyone it shouldn't be.

When we use third party organisations to process information on our behalf we ask them to demonstrate their compliance with our security requirements, and any instructions we may give them and their compliance with relevant data protection legislation throughout the time they work for DAN. These organisations take their instructions from us, and their obligations regarding what information they process and what they can do with it are agreed in the contracts we have with them.

Any questions?

If you have any questions or queries about the way in which we process your personal data please contact either your local HR Recruitment Team, or the Global Data Protection Officer – DPO@dentsuaegis.com

Status of this Privacy Notice and notification of changes

We may update this Privacy Notice at any time but will be reviewed annually.

This Privacy Notice was last updated and reviewed on 16th March 2018.



Definitions

Word or phrase	What does it mean?
DAN organisation	The specific DAN entity that entered into an employment contract or relationship or a contract for services with you.
Data controller	<p>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.</p> <p>This will be the DAN organisation that entered into an employment agreement or contract for services with you. It may also include other DAN organisations that need to process your personal data for their own purposes.</p>
Other DAN organisations	The parents, affiliates, and/or subsidiaries of the DAN organisation described above.
Personal data	<p>Any information relating to an identified or identifiable person. An identifiable person is someone who can be identified, directly or indirectly, by reference to details such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</p> <p>Personal data includes the data that's described in the section of the Privacy Notice called What type of personal data do we collect about you?</p>
Processing (or Processed)	Any operation which is performed on personal data - 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.
Special Categories / Sensitive personal data	<p>Personal data that may reveal sensitive matters such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and also includes genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or sex life or orientation.</p> <p>Sensitive personal data includes the data that's described in the section of the Privacy Notice called What type of personal data do we collect about you</p>
Supervisory authority	The authority responsible for dealing with data protection. In the UK, for example, this would be the Information Commissioner's Office.

