

(INTERNAL PLATFORM) DATA PRIVACY NOTICE FOR CANDIDATES

IDIADA Automotive Technology UK Ltd is committed to protecting the privacy and security of your personal information.

This Privacy Notice describes how we collect and use personal information about you during and after your relationship with us, in accordance with data protection law.

It applies to all candidates.

Purpose Of This Privacy Notice

IDIADA AUTOMOTIVE TECHNOLOGY UK LTD (“the Company”) is a “data controller”. This means that we are responsible for deciding how we hold and use personal and certain information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to candidates and prospective candidates who register with us for roles at IDIADA,. We may update this notice at any time but, if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

This notice makes you aware of how and why your personal data will be used, namely for the performance of the contract of employment/engagement, for how long it will usually be retained together with your rights under the data protection legislation. It provides you with certain information that must be provided pursuant to the general data protection legislation that is applicable (“Relevant Privacy Legislation”) in particular the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Key Principles

We will comply with Relevant Privacy Legislation, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Information Held

Personal Data is any data from which you can be identified (“Personal Data”). Such data can be sensitive where it concerns sensitive information (now called “Special Categories of

Personal Data”). For the purposes of this notice, Personal Data and Special Categories of Personal Data together constitute “Relevant Data”.

Personal Data does not include data where your identity has been removed (anonymous data).

In connection with your contract of employment/engagement with us we will collect, store and use any or all of the following categories of personal information about you:

- Your personal details such as your name, address, telephone number, mobile number, email address, date of birth, sex, marital status, nationality and ethnicity.
- Data from use of our website, platform, links in emails we may send to you or job alerts or other content from us, we also collect personal data from those interactions.
- Details regarding your emergency contacts and any beneficiaries, where relevant.
- Details concerning your health, health and sickness records or assessments, any occupational health or other expert report we may require and any other personal background (such as whether you are married and have caring responsibilities). Some of this information may constitute special category data (see below).
- Information pertaining to any criminal convictions, charges or otherwise as well as your credit worthiness / debt position and transactions you may have agreed with the Company such as a loan. Some of this information may constitute special category data (see below).
- Recruitment information such as references, CVs, assessment notes and test scores, verification checks, Disclosure and Barring Service Checks, right to work in the UK documentation and equal opportunities monitoring forms and photographs.
- Written particulars of employment or engagement, documented changes to terms and conditions or working time opt outs.
- Any past or current collective agreements that could affect you.
- Information for payroll or invoicing purposes such as PAYE records, current bank details, wage records and slips (including salary, bonuses and payments in kind), tax status, NI number, P45s, P60s, hours worked (including overtime) and any travel/mileage or expenses claimed, advances or loans, as well as whether you are solvent.
- Details concerning your pension and any other benefits including nomination and revocation forms and who should benefit from your pension or other benefits, if applicable.
- Your driving licence, insurance details and other documentation which may affect your ability to work or has an impact on equipment or goods we may supply, which we or you may be required to insure.
- The work you are required to undertake, or services you provide, as part of your role (and any work done, reports or records arising out of your role with the Company) as well as your recruitment information, employment/engagement records, start date,

location of employment/engagement or workplace, annual leave or other absences, any disciplinary, grievance, sickness records and other related matters such as qualifications, training and compensation package.

Records to show compliance with our legal obligations including time sheets and health and safety assessments.

- Information we have obtained, directly or otherwise, through social media or other means. This includes your use of any electronic communications we have supplied together with any other equipment in addition to photographs, CCTV footage and swipe cards.
- Identifying trends so that measures can be put in place, for instance, to improve our operations.
- Details pertaining to resignation, termination, redundancy or retirement.
- Any other pertinent information that is necessary for the purposes of your employment/engagement, or otherwise arising out of a request made by you.

We may also collect, store and use the following Special Categories of Personal Data pertaining to you:

- Information about your race or ethnicity, religious beliefs, sexual orientation, political opinions and memberships.
- Information about your health including any medical condition, health and sickness records, genetic and/or biometric data. This may also include details relating to your leaving employment and any share plan operated by a group company where the reason for leaving is determined to be ill health, injury or disability, along with the records relating to that decision.
- Data relating to any trade union membership.
- Genetic information and biometric data, if applicable.
- Information about criminal convictions and offences, if applicable.
- Information about you leaving employment where the reason for leaving is related to your health, including information about that condition needed for pensions and permanent health insurance purposes.

Data Sources

Apart from obtaining any of your Relevant Data directly from the individual we may collect We collect personal information about ,prospective candidates, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may also collect profession biographical details obtained from publicly available sources such as LinkedIn and social media sites. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies (including the Disclosure and Barring Service in respect of criminal convictions, where we are entitled and/or required to do so in light of the particular role), trustees/managers of pension arrangements and/or data from any publicly accessible source including social media and LinkedIn.

We will collect additional personal information in the course of job related activities throughout the period of you working for, or providing services to, us.

How Relevant Data Is Used

We will use Relevant Data we collect about you to be able to:

- Administer the employment or engagement contract we have entered into with you.
- Assess your skills, qualifications, and suitability for any work or services as well as checking you are legally entitled to work in the UK and in any role.
- Ensure we have addressed any safeguarding measures.
- Make decisions about your future or ongoing employment/engagement and its termination.
- Determine the terms on which you can work for or provide services to us and on what basis a reference could be supplied.
- Liaise with any third party providers such as payroll and Occupational Health for administration purposes.
- Comply with legal and regulatory requirements as well as managing our legal obligations including compliance in preventing fraud and bribery and/or health and safety matters, as well as investigating and providing evidence where relevant.
- Determine accreditation or professional membership(s).
- Ensure our network(s), and information held on them, is/are secure to the extent reasonably possible to prevent any accidental or unlawful leak, access or other.
- Enable us to monitor trends and introduce or revise any practices we adopt such as regarding equal opportunities.
- Identify causes for and otherwise in relation to the purposes of corporate social responsibility.
- Establish and improve any product and service we could supply to you or others (such as discounted services).
- Deal with legal disputes involving you.

It is in any event in our legitimate interests to hold Relevant Data when you work for us.

Whilst it is rare, there may be times where Relevant Data is processed for the purposes of protecting your interests, that of a third party or where there is a need to do so for public interest reasons or for official purposes. An example would include a potential or actual crime taking place which relates to your Relevant Data.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

How We Use Particularly Sensitive Personal Information

"Special categories" of personal information, such as information about your health, racial or ethnic origin, sexual orientation or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.
- Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Situations In Which We Will Use Your Sensitive Personal Information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment/engagement. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so.

The situations in which we will process your particularly sensitive personal information are listed below:

- We may use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and any insurance.
- We may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

If You Fail To Provide Personal Information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to in respect of health and safety).

Change Of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Do We Need Your Consent?

We do not need your consent if we use your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your wellbeing and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. You will not be subject to decisions that will have a significant impact on you based solely on automated and/or biometric decision making, unless we have a lawful basis for doing so and we have notified you.

Data Sharing

We will only share your personal information with third parties for the performance of your contract of employment or engagement with us and/or where there are other legitimate reasons to do so. This may include:

- Any group company of IDIADA AUTOMOTIVE TECHNOLOGY UK LTD (including any parent, subsidiary, investee or affiliate company).
- Any payroll, pension and/or benefits provider or administrator.
- Consultants and companies that assist the Company from an IT and infrastructure point of view.
- Professionals, service consortia and consultants who assist the Company from a fiscal, commercial, legal and medical point of view.
- Banks and other credit institutions.

- Judicial offices, police and armed forces.

All our third party service providers and other entities in the group are required to take appropriate security measures to protect your Relevant Data in line with our policies. We do not allow our third party service providers to use your Relevant Data for their own purposes. We only permit them to process your Relevant Data for specified purposes and in accordance with our instructions.

Where we have shared any of your Relevant Data with a third party they are required to take appropriate security measures to protect such information. Such parties are only able to process that data in accordance with our instructions. There may also be the need for us to share your Relevant Data in respect of any business reorganisation, restructure, buy out or otherwise that may need to take place.

In terms of our obligation to deal with regulatory matters, accreditation or professional membership or other matters we will where necessary share any of your personal data that we hold.

Where there is any associated company any Relevant Data pertaining to you that we hold will be shared with any such business as and where appropriate.

Transferring Relevant Data

We have put in place systems whereby your Relevant Data will be held in the UK.

Data is stored and hosted in servers in both the UK and the European Union and may be locked and encrypted, if necessary. Access to Relevant Data is limited to key personnel and protected such as via a password. Where any data is stored on company property, such as on laptops, both the hardware and software will have appropriate protections in place.

The data may be stored electronically and in physical form, including on cloud based and other storage platforms. You should be aware that devices may obtain access to other records, such as personal photographs on your device if you use our computers to charge your mobile phone. If for any reason another storage system is used and placed outside the areas mentioned we will use reasonable measures to ensure there is an adequate level of protection of your personal information.

If there has been a breach of any Relevant Data that concerns you and may result in a high risk to your individual rights and freedoms, you will be informed accordingly. We also have an obligation to notify the regulatory body (including the Information Commissioner's Office ("ICO") referred to below) and any other appropriate party.

Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way or otherwise altered or disclosed. Additionally, we limit access to your Relevant Data to those candidates, who have a business need to know. They will only process your Relevant Data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you, and any applicable regulator, where we are legally required to do so.

Data Retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In the majority of cases, it is expected that we will retain personal data throughout the period of your employment/engagement and for up to 5 years thereafter. In some cases extremely limited cases, we may be required or entitled to retain certain personal data for a longer period. Some personal information, such as bank details, will be deleted shortly after your employment/engagement ends and any final payments have been made.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer a candidate we will securely destroy your personal information in accordance with applicable laws and regulations.

Rights

Under certain circumstances, by law you have the right to:

- Request access to your Relevant Data (commonly known as a “data subject access request”). This enables you to receive a copy of the Relevant Data we hold about you and to check that we are lawfully processing it.
- Request correction of the Relevant Data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your Relevant Data. This enables you to ask us to delete or remove Relevant Data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Relevant Data where you have exercised your right to object to processing (see below).
- Object to processing of your Relevant Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your Relevant Data. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your Relevant Data to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Company’s Data Protection Manager in writing.

No Fee Usually Required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What We May Need From You

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right To Withdraw Consent

Where you have provided your consent to the Company to process your personal information for a specific purpose, you do have the right to withdraw your consent for that particular processing at any time. To withdraw your consent please contact the Company's Data Protection Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Contact Points

We have appointed Mr. Albert Vives as our Data Protection Manager to oversee compliance with this Privacy Notice.

If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Manager at any of the following:

Name: Albert Vives
Headquarter: St Georges Way Bermuda Industrial Estate CV10 7JS Nuneaton United Kingdom
Telephone: +44 2476 328 083
Email: data_protection@idiada.com

If at any time you wish to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues, you can do so.

ACKNOWLEDGEMENT OF UNDERSTANDING

I acknowledge that I have received a copy of the IDIADA Automotive Technology UK Ltd Privacy Notice for candidates, and that I have read and understood it.

Signature

Printed Name

Date.....