AI Digital Contracts Inc. Privacy Policy

AI Digital Contracts Inc. Privacy Policy Overview

AI Digital Contracts Inc. and its international subsidiaries respect your privacy and are committed to protecting your Personal Data. As a global organization, it is our duty to comply with the various applicable regulations around the world that govern the collection and processing of Personal Data.

Protecting the personal rights and privacy of each individual is at the core of the foundation of trust in our business relationships and of Axiom's reputation as an attractive and responsible employer. We recognize the need for appropriate safeguards and management practices in relation to the collection and use of your Personal Data.

We want to ensure that you understand what information we collect about you and how we use it. This Privacy Policy sets out the principles Axiom follows when we collect and process your Personal Data through your use of our website or when you otherwise engage with Axiom and it applies to our candidates, clients, suppliers, website-users and anyone who subscribes to our newsletters or participate in our programs or similar activity.

This website is not intended for children and we do not knowingly collect data relating to children.

We may amend this Privacy Policy from time to time, and we will endeavor to inform our contacts of major changes to this policy. You may always review our current policy at this page. If we need your consent to process your Personal Data in a different way, we will seek your permission in advance.

Please use the Glossary to help you understand the meaning of some of the terms used. If you have any questions regarding the policy, contact us at aidcprivacy@axiomlaw.com.

1. WHO WE ARE

AI Digital Contracts Inc.
AI Digital Contracts Inc. ("AIDC") is a leading alternative legal services provider headquartered at 295 Lafayette Street New York, New York 10012, USA. AIDC is the parent company of several entities, including:

- **AI Digital Contracts Services Ltd,** a *UK Company*
- **AI Digital Contracts SP.zo.o**, a *Polish Company*

This Privacy Policy is issued on behalf of AIDC as a whole. When we mention "AIDC", "we", "us" or "our", we are referring to the relevant AIDC entity responsible for collecting or processing your data.

Unless specified otherwise in this Privacy Policy, AIDC is the controller of your Personal Data which means that AIDC decides why and how your Personal Data is processed. Unless otherwise stated the AIDC entity you are engaging with will be the controller of your data. AIDC is the controller and responsible for this website.

AIDC was established in February 2019 through spin-off (the "Spin-Off") of a business unit of Axiom Global Inc. ("Axiom"). For a limited period of time, some of the processing of personal data described in this Privacy Policy, primarily for administrative purposes, will be handled by Axiom on behalf of AIDC, as described below under "How We Share Your Personal Data". Following the Spin-Off and subsequent legal transfer of client contracts, processing of client data for performance of services under client contracts will generally be performed by AIDC itself.

Data Privacy Office
Our Data Privacy Office, which is part of our Legal & Compliance team, is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise any of your legal rights, please contact the Data Privacy Office using the details set out below.

Contact Details
Our full details are:

Full name of legal entity: AI Digital Contracts Inc.

Address: 295 Lafayette Street, Suite 700
New York, NY 10012

Contact Name: Alec Guettel

Email address: aidcprivacy@axiomlaw.com

Telephone number: +1.917.237.2900

2. WHAT PERSONAL DATA WE COLLECT AND HOW WE COLLECT IT

"**Personal Data**" is any information about an individual from which that person can be identified. It might include your name, mailing address, email address, telephone number, company, title, site username or site password. It does not include data where the identity has been removed (anonymous data).

We collect, store and process your Personal Data by different methods depending on whether you are a candidate, client, supplier or website user.

WHERE YOU ARE A CANDIDATE:
You may be a past candidate or a candidate in process or you may have participated in our recruitment or other similar events.

- How we collect your data:
  - You may provide Personal Data to us by email, post, telephone, face to face during meetings or at our events or through our website; or
  - We may collect your data indirectly or from third parties: through recruitment agencies, social media searches (such as LinkedIn), research companies, client or supplier conversations, or referrals from other third parties.
- What data we collect:
  - The Personal Data we collect about candidates includes: first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender, right to work, social security/national insurance number, nationality, employment and education history, skills proficiency, references, or qualifications information contained in your resume/CV, or written records of our conversations or meetings.

We do not mandate the collection of any **Special Categories** of Personal Data about you through this website (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data).

We will ask for your **explicit consent** before we collect Special Category Personal Data, except in circumstances:

- where required by law;
- for employment purposes; or
- where required to carry out criminal or other background checks.

WHERE YOU ARE A CLIENT:
When you are inquiring about or using our services we collect and use information to understand your requirements, agree role specifications, propose candidates, discuss our contract, provide training or consultancy services or to share AIDC content which is likely to be relevant and useful to you.

- How we collect your data:
  - You may provide Personal Data to us by email, post, telephone, face to face during meetings or through our website; or
  - We may collect it from your colleagues, social media, our network of contacts, others who may know you, event delegate lists or third-party market research.
- What data we collect:
  - Data we collect includes the Personal Data of individual contacts who we deal with at your organization such as: name, job title, management level, business relationships, memberships, work history, work address, telephone numbers, and email address or written records of our conversations or meetings.

WHERE YOU ARE A SUPPLIER:
When supplying services to us or contracting with us we need certain information so that we can receive and pay for the services you provide.

- How we collect your data:
  - You may provide Personal Data to us by email, post, telephone, face to face or to our website; or

- We may collect it from candidates, social media, from our network contacts / others who may know you, event delegate lists or third-party market research.

- What data we collect:
  - This includes the Personal Data of individual contacts we engage with at your organization such as: name, job title, work address, telephone numbers, email address or written records of our conversations or meetings.

WHERE YOU ARE A WEBSITE USER:
When you are using our website, which may include when you download content or contact us via our website.

- How we collect your data:
  - You may provide Personal Data by completing online registration forms, by applying for roles via our website, or when you create or update any of your marketing preferences;

  - We may collect your data automatically via cookies, in line with cookie consent, server logs and other similar technologies preferences and settings in your browser; or

  - For more information on how we use cookies please see our cookie policy.

- What data we collect
  - We collect the information you provide which may include your name and contact details, email address and telephone number, the resume/CV you submitted it to us online. In addition, we collect a limited amount of data which we use to help us to improve your experience when using our website and to help us manage the services we provide. This includes information on how you use our website and the location you view our website from (IP address).

3. HOW WE USE YOUR PERSONAL DATA

We collect, process or disclose your Personal Data for our legitimate business purposes including:

- To provide our services to clients, candidates or web users or to fulfill our contractual obligations;
- To maintain our business relationships;
- To match candidate details with client requirements for roles and to send candidates' Personal Data which may include special category data to clients to fill those roles;
- To notify candidates of roles which we feel would be of interest to them;
- To provide candidates with HR related support and services;
- To market events, promotions, competitions, webinars, reports, our services, news or relevant industry updates. Depending on which jurisdiction you are in, we may be required to give you an option to "opt-in" and we will always provide you with an option to "opt-out" with each marketing communication;
- As required by law or regulation;
- For our business purposes, such as data analysis, audits, fraud monitoring and prevention;
- To develop new products, services and offerings, or to enhance, improve or modify our products and services; or
- To record your usage of our website in accordance with our cookie policy.

Pursuant to our contractual obligations with clients and customers, AIDC may engage in automated processing of data under client contracts, which may include personal data. Only AIDC clients, and never AIDC, engage in individual decision-making or profiling as a result of such processing.

4. WHAT IS THE LEGAL BASIS FOR PROCESSING YOUR DATA

We rely on the following main grounds to process Personal Data of candidates, clients, suppliers, web users or other third parties:

- **Necessary for entering into, or performing, a contract** – to perform obligations that we undertake in providing a service to you, or to take steps at your request to enter into a contract with us;

- **Necessary for compliance with a legal obligation** – we are subject to certain legal requirements which may require us to process your Personal Data. We may also be obliged by law to disclose your Personal Data to a regulatory body or law enforcement agency;

- **Necessary for the purposes of Legitimate Interests** – we, or a third party, will process your Personal Data for the purposes of our (or a third party's) Legitimate Interests, provided we have established that those interests are not overridden by your rights and freedoms, including your right to have your Personal Data protected. Our Legitimate Interests include responding to requests and enquiries from you or a third party, optimizing our website and customer experience, informing you about our products and services and ensuring that our operations are conducted in an appropriate and efficient manner;

- **Consent** – in some circumstances, we may ask for your consent to process your Personal Data;

- **Necessary to protect the vital interests** of the data subject or of another natural person.

CHANGE OF PURPOSE

We will only use your Personal Data 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 you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at aidcprivacy@axiomlaw.com.

If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so or seek your consent, providing you with a clear, conspicuous and readily available mechanism for you to exercise choice.

Please note that we may process your Personal Data without your knowledge or consent where this is required or permitted by law.

5. HOW WE SHARE YOUR PERSONAL DATA

We will not sell or rent to anyone the Personal Data provided to us or obtained by us.

In certain circumstances we will share your Personal Data with other parties.

We share your data with other entities within AIDC acting as joint controllers or processors. We do this to provide sales and marketing, IT, HR, system administration services, product development and undertake internal reporting. We will also share your Personal Data across AIDC entities to provide candidates to our clients to fulfill client engagements, for business development, to improve our client service and to make our services more valuable to you.

For a limited period of time, as a result of the Spin-Off, we will also share your data with Axiom, Ardent Managed Solutions Inc. (which was spun off from Axiom at the same time as the Spin-Off) and their subsidiaries, under transition services agreements that ensure the same high degree of privacy and confidentiality for your data as applied prior to the Spin-Off. Specifically, Axiom will process AIDC administrative data, including for IT, HR, and systems administration purposes, until the end of 2019 (or earlier); and Ardent Managed Solutions Inc. will share certain staff and support with AIDC, including providing client delivery services and receiving systems management, for up to six months after the Spin-Off. Over the course of 2019, these functions are expected to be transitioned to permanent arrangements for handling of your data by AIDC.

We also share your Personal Data with the following third parties:

- Service providers acting as processors who provide IT and system administration services, including Salesforce, Workday, OpenAir and Bullhorn;
- Professional advisers acting as processors or joint controllers;
- Regulators and other authorities acting as processors or joint controllers based who require reporting of processing activities in certain circumstances. Clients who have roles in which you are interested;
- Trusted third parties who provide employment related services for us, including reference, qualification, and criminal record checking (where required), evaluation or skills tests. In such circumstances we may disclose Special Category data; or
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. If a change happens to our business, then the new owners may use your Personal Data in the same way as set out in this Privacy Policy.

We require all third parties to respect the security of your Personal Data and to treat it in accordance with applicable laws. We do not allow our third-party service providers to use your Personal Data for their own purposes and only permit them to process your Personal Data for specified purposes and in accordance with our instructions.

We also collect, use and share aggregated data such as statistical or demographic data for purposes which include monitoring how we are doing against our Diversity and Equality targets. Aggregated data is not Personal Data as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Personal Data where we are required by law to report on mixes of religious beliefs or political opinions or affiliations.

6. INTERNATIONAL TRANSFERS OF DATA

We share your Personal Data within AIDC. We transfer the Personal Data we collect about you to countries outside of the country in which the information originally was collected. Those countries may not have the same data protection laws as the country in which you initially provided the information. When we transfer your information to other countries, we will protect that information as described in this Privacy Policy.

Transfers out of the EEA

If you are located in the European Economic Area (EEA) this may involve transferring your Personal Data outside of the EEA. Whenever we transfer your Personal Data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented.

General Safeguards

- We will only transfer your Personal Data to countries that have been deemed to provide an adequate level of protection for Personal Data by the European Commission. For further details, see *European Commission: Adequacy of the protection of Personal Data in non-EU countries*.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give Personal Data the same protection it has in Europe. For further details, see *European Commission: Model contracts for the transfer of Personal Data to third countries*.

EU-US Privacy Shield Framework

- Where we transfer data to AIDC in the US or use third party providers in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to Personal Data shared between the Europe and the US. For further details, see *European Commission: EU-US Privacy Shield*. To learn more about the Privacy Shield program, and to view our certification page, please visit www.privacyshield.gov
- AIDC commits to cooperate with EU data protection authorities and comply with the advice given by such authorities on human resources data transferred from the EU in the context of the employment relationship.
- AIDC certifies that it complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, retention, and transfer of Personal Information from EU. member countries to the United States, respectively.
- AIDC further certifies that it adheres to the Privacy Shield Privacy Principles of 1) Notice, 2) Choice, 3) Accountability for Onward Transfer, 4) Security, 5) Data Integrity and Purpose Limitation, 6) Access, and 7) Recourse, Enforcement, and Liability.
- If there is any conflict between this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles will govern. To learn more about the Privacy Shield program, and to view our certification page, please visit the following URL: https://www.privacyshield.gov/
- AIDC is subject to the jurisdiction, enforcement, and investigatory authority of the United States Federal Trade Commission as well as EU, Hong Kong, and Singapore data protection authorities.
- Further, AIDC commits to cooperate with EU, Hong Kong, and Singaporean data protection authorities (DPAs) and comply with the direction given by such authorities on other information transferred from these countries / jurisdictions.

Please contact us at aidcprivacy@axiomlaw.com if you want further information on the specific mechanism we use when transferring your Personal Data out of the EEA.

7. DATA SECURITY

AIDC uses industry standard physical, technical, and administrative controls to protect your Personal Data by:

- Not collecting or retaining excessive amounts of data;
- Protecting Personal Data from loss, misuse, unauthorized access and disclosure. Any employees, agents, contractors or third parties who are so authorized act on our instructions and are subject to a duty of confidentiality;
- Keeping Personal Data up to date;
- Storing and destroying it securely;
- Ensuring that appropriate administrative, technical and physical safeguards are in place to protect Personal Data. These measures include measures to deal with any suspected data breach; and
- Regularly reviewing our information collection, storage and processing practices, including physical security measures.

While we operate to the highest standards we are also aware that the transmission of information via the internet is not completely secure. We cannot guarantee the security of your data transmitted to our website and any transmission is at your own risk. Where we have given you (or where you have chosen) a password which enables you to access any of our online or electronic resources, you are responsible for keeping this password confidential. We advise you not to share your password with anyone.

You should note that this website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their content or privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Cookies

AIDC uses "cookies" on its sites. A cookie is a piece of data stored on a site visitor's system that help us improve your access to our site and identify repeat visitors to our site.

Cookies can also enable us to track and target the interests of our users to enhance their experience on our site. Except where 1) contacts elect to identify themselves for purposes of receiving information from AIDC or inquiring as to a business relationship with AIDC or 2) candidates elect to establish and use an account to apply to AIDC and employment opportunities with AIDC, cookies are not linked to any personally identifiable information.

You can disable or remove any cookies already stored on your computer, but these may stop our websites from functioning properly.

8. DATA RETENTION

Where we collect your Personal Data, the length of time for which we retain it depends on the type of data, the purpose for which we use that data and our accounting, regulatory and legal data retention obligations. We do not retain Personal Data in an identifiable format for longer than:

- The period necessary for the relevant activity or services;
- Any retention period that is required by law or contract; or
- The period in which litigation or investigations might arise in respect of the relevant activity or services

After which, it is likely your Personal Data will no longer be relevant for the purposes for which it was collected and we will delete or destroy it.

In some circumstances we may anonymize your Personal Data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

9. YOUR LEGAL RIGHTS

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

- **Request access to your personal information** (commonly known as a "subject access request" or "SAR"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- **Request correction of the personal information** that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information 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 personal information where you have exercised your right to object to processing. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request;
- **Object to processing** of your personal information 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 personal information**. 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; and/or
- **Request the transfer of your personal information** 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 us by email at aidcprivacy@axiomlaw.com.

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

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please send us email at aidcprivacy@axiomlaw.com. 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 legal basis for doing so.

Our response timescales

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is incomplete and we need to write to you for more information or is particularly complex or you have made several requests. In these case, we will notify you and keep you updated.

The right to complain to a supervisory authority

In the EU we have nominated the UK Supervisory Authority as the Lead Supervisory Authority for our EU based establishments (Poland, UK). You have the right to complain to the Information Commissioner's Office about how and/or why we are processing your Personal Data.

You also have a right to make a complaint regarding how and / or why we process your data with respect to the EU-US Privacy Shield Principles.

Please see “how to make a complaint”.

10. HOW TO MAKE A COMPLAINT

Data privacy laws are constantly evolving and we endeavor to maintain best practice. However, we recognize that we may not always get it right and if you are not satisfied in the way we handle your Personal Data or you wish to discuss our processes then we would like to hear from you.

AIDC Complaint process

If there is something which we have not done correctly with your Personal Data then we would appreciate the chance to deal with your concerns before you approach a Supervisory Authority so please contact us in the first instance – aidcprivacy@axiomlaw.com.

EU Supervisory Authority

In any case, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (*www.ico.org.uk*).

In the EU we have nominated the ICO as the Lead Supervisory Authority for our EU based establishments (Poland, UK). You have the right to complain to the Information Commissioner's Office about how and/or why we are processing your Personal Data for any of our European Entities.

EU-US Privacy Shield

In compliance with the EU-US Privacy Shield Principles, AIDC commits to resolve complaints about 1) your privacy and 2) our collection or use of your personal information. EU individuals with 1) inquiries or complaints regarding our Privacy Shield policy or 2) questions or concerns about the use of their Personal Information should first contact AIDC at aidcprivacy@axiomlaw.com.

AIDC has further committed to refer unresolved Privacy Shield complaints to TrustArc, an alternative dispute resolution provider headquartered in both the EU and the US. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact or visit TrustArc for more information or to file a complaint at: https://www.trustarc.com/consumer-resources/dispute-resolution/.

The services of TrustArc are provided at no cost to you.

If your complaint is not resolved after following the recourse mechanisms described above, you may have the ability to invoke binding arbitration. More information can be found at the following URL: http://go.adr.org/privacyshieldfiling.html

11. GLOSSARY

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organization that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Data for our legitimate interests. We do not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category (Sensitive) Personal Data and pseudonymized Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behavior.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when AIDC collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Category or Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offenses and convictions.