



SEC-02

Privacy Policy

Kyron Intelligence | Privacy Notice

Policy ID	SEC-02
Version	1.0
Document Owner	CEO
Approver	CEO
Classification	PUBLIC
Status	Approved
Effective Date	15-Sep-26
Review Date	15-Sep-27
Review Frequency	Annual
Website	www.kyronintelligence.com

1. Introduction and Purpose

This Privacy Policy explains how Kyron Intelligence Ltd collects, uses, shares, protects and retains personal data when delivering intelligence, search, operational, consulting and assessment services, when engaging with candidates, clients, referees and business contacts, and when individuals use our website or receive communications from us. We are committed to privacy by design and default, data minimisation, transparency and appropriate security.

2. Who We Are

Kyron Intelligence Ltd (we, us, our) is responsible for determining how personal data covered by this notice is processed where it acts as controller. Information about our services is available at www.kyronintelligence.com. Privacy enquiries and rights requests may be sent to cl@kyronintelligence.com. The CEO has overall responsibility for privacy and data protection governance.

3. Who This Notice Applies To

- Candidates, applicants, and potential candidates.
- Client personnel and prospective clients.
- Referees.
- Suppliers, consultants, and professional contacts.
- People who attend our events, request information, subscribe to communications, or interact with us online.
- Website visitors and other individuals whose personal data we process in connection with our legitimate business activities.

Separate workforce privacy information may apply to employees, workers, and other personnel.

4. Personal Data We May Collect

- Identity and contact information, such as name, address, telephone number, and email address.
- Professional information, including role, employer, CV or resume, employment history, education, professional qualifications, memberships and references.
- Information supplied by clients, referees, or sources about professional experience, relationships, or suitability.
- Communications, preferences, enquiries, event attendance, and records of interactions with us.
- Website and technical information, such as device, log, cookie or analytics information collected.
- Due-diligence, screening or vetting information where relevant and lawful.
- Special category or criminal offence data only where necessary, lawful and subject to the additional safeguards required by data protection law.

5. How We Obtain Personal Data

We may obtain personal data directly from you, from organisations or individuals you authorise us to contact, from clients, referees or sources, from service providers, and from lawful publicly available sources. Where we obtain personal data indirectly, we will provide privacy information where required, subject to any applicable legal exemptions.

6. Purposes and Lawful Bases

We process personal data only where we have an appropriate lawful basis. Depending on the activity, this may include taking steps at your request before entering into a contract, performance of a contract, compliance with a legal obligation, or a third party's legitimate interests where those interests are not overridden by your rights, or consent where consent is the appropriate basis. Examples of purposes include:

- Assessing and discussing potential employment, consultancy, or assignment opportunities.
- Delivering client intelligence, search, consulting, assessment and related professional services.
- Managing client, supplier, and business relationships.
- Conducting lawful research, market mapping, and professional sector analysis.
- Performing appropriate due diligence, screening, and vetting.
- Operating, securing and improving our systems, websites and services.
- Managing events, enquiries, communications, and permitted marketing.
- Establishing, exercising or defending legal claims and meeting legal, regulatory, audit and security obligations.

7. Candidates

Where you apply for or discuss an opportunity, we may process professional, contact, career and assessment information to evaluate suitability, communicate with you, arrange interviews or assessments, obtain authorised references, and present relevant information to an appropriate client or decision-maker. Where vetting or security clearance is required, only necessary information will be shared with authorised providers or bodies under an appropriate lawful basis and safeguards.

8. Clients, Sources and Referees

For client contacts we may process contact details, role information, correspondence and information necessary to manage our services and relationship. For sources and referees we may process contact information, professional credentials, relationship to a candidate or matter, and information or opinions supplied to us. We will handle source and referee information proportionately and apply confidentiality and security restrictions where appropriate.

9. Special Category and Criminal Offence Data

We do not seek sensitive personal data unless it is relevant and lawful to process. Where special category data or criminal offence data is required, we will identify an appropriate legal basis and additional condition, apply

enhanced access and handling controls, and provide appropriate information to the individual. Consent will not be used automatically where another lawful basis or statutory condition is more appropriate.

10. Sharing Personal Data

We may share the minimum necessary personal data with authorised recipients where there is a lawful purpose, including:

- Clients or prospective clients where necessary to provide an agreed service or progress an authorised opportunity.
- Vetting, screening, assessment or professional-service providers where appropriate.
- IT, hosting, communications, analytics, customer-support and other suppliers acting under appropriate contractual and security requirements.
- Professional advisers, auditors, insurers or corporate advisers where necessary.
- Law enforcement, courts, regulators or public authorities where disclosure is required or otherwise lawful.

Where another organisation processes personal data on our behalf, we require appropriate contractual, confidentiality and security controls. Where the recipient acts as an independent controller, it is responsible for its own data protection obligations.

11. International Transfers

Where personal data is transferred outside the UK in circumstances governed by international-transfer rules, we will assess the transfer and use an applicable lawful mechanism, such as UK adequacy regulations, appropriate safeguards or a permitted exception. Additional contractual, risk-assessment and security measures will be used where required.

12. Retention

We retain personal data only for as long as reasonably necessary for the purpose for which it was collected and to meet applicable legal, regulatory, contractual, tax, accounting, security or dispute-management requirements. Retention is based on the category of information and purpose, not simply on whether consent remains available. When information is no longer required, it will be securely deleted, destroyed or anonymised in accordance with our retention requirements.

13. Your Data Protection Rights

Depending on the circumstances, you may have rights to request access to your personal data, correction of inaccurate data, erasure, restriction of processing, objection to processing, data portability, and safeguards in relation to certain automated decision-making. Where processing relies on consent, you may withdraw that consent without affecting processing already carried out lawfully. These rights are not absolute and applicable legal exemptions may apply.

14. Exercising Your Rights

You may exercise your rights by contacting cl@kyronintelligence.com. We may ask for information reasonably necessary to confirm identity and locate the relevant data. We will respond without undue delay and normally within one month of receiving the request. Where permitted by law, this period may be extended by up to a further two months for complex or multiple requests, and we will explain the extension within the initial period. Information will be provided securely.

15. Direct Marketing and Communications

Where we send newsletters, role alerts or other direct marketing, we will use an appropriate lawful basis and comply with applicable electronic-marketing requirements. You can unsubscribe or change your preferences at any time using the method provided in the communication or by contacting us. Withdrawal from marketing will not prevent necessary service, legal, security or administrative communications.

16. Website, Analytics and Cookies

Our website at www.kyronintelligence.com may use cookies and other storage or access technologies to operate the service, maintain security, understand usage and improve functionality. We will provide clear information about relevant technologies. Where prior consent is legally required for non-exempt technologies, they will not be enabled before valid consent is obtained. Users should be able to make appropriate choices and withdraw or change consent through the available website controls. Blocking some technologies may affect website functionality.

17. Security

We use proportionate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures may include access control, multi-factor authentication, encryption, system hardening, logging, monitoring, backups, personnel controls and supplier security requirements. No system can eliminate all risk, but we maintain controls appropriate to the nature of the information and the threats reasonably anticipated.

18. Information About Other People

If you provide personal data about another person, such as a referee or professional contact, you should only do so where you are entitled to provide it. We will determine our own lawful basis for any processing we undertake and will provide privacy information to that person where required. We do not rely solely on a third party obtaining consent on our behalf unless consent is genuinely the appropriate basis.

19. Automated Decision-Making

We do not currently make solely automated decisions about individuals that produce legal or similarly significant effects as part of the processing described in this policy. If this changes, we will provide the information and safeguards required by applicable data protection law.

20. Third-Party Websites

Our website may contain links to websites operated by other organisations. This Privacy Policy does not govern those external websites. You should review the privacy information provided by the relevant third party before providing personal data.

21. Complaints

If you have concerns about our use of your personal data, please contact us first at cl@kyronintelligence.com so that we can investigate. You also have the right to complain to the Information Commissioner's Office where you consider that your data protection rights have been infringed. Further information is available at www.ico.org.uk.

22. Changes to This Policy

We keep this Privacy Policy under review and will update it when our processing activities, legal requirements, services or technology materially change. The current version and effective date should be made available through the appropriate Company channel and, where relevant, our website.

23. Related Documents

- SEC-01 Data Protection Policy
- SEC-03 Information Security Policy
- SEC-04 Access Control and Identity Management Policy
- SEC-05 Data Classification and Handling Policy
- SEC-09 Incident Response and Breach Management Policy
- SEC-14 Third Party and Suppliers Policy
- SEC-16 Data Retention and Secure Disposal Policy
- HR-03 Employee Privacy Notice

24. Approval

Role	Name	Position	Date
Owner	Christopher Lowry	CEO	15 Sept 26
Approver	Christopher Lowry	CEO	15 Sept 26

25. Document Control

Version	Date	Change	Approved By
1.0	15-Sep-26	Initial controlled issue	CEO