PRIVACY NOTICE

How We Use Your Personal Information

---

1. Introduction

M4 Digital Group Ltd ("M4", "we", "us" or "our") is committed to protecting and respecting your privacy.

This Privacy Notice explains how we collect, use, store, share and protect personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and the Data (Use and Access) Act 2025 (DUAA). These laws govern how organisations collect, use, protect and manage personal information. [gov.uk], [ico.org.uk]

This notice applies to:

- Visitors to our website
- Prospective and existing customers
- Suppliers and business contacts
- Job applicants
- Employees, contractors and consultants
- Individuals whose personal information is provided to us during the course of our business activities

By engaging with M4 Digital Group Ltd, using our services, submitting information to us, or visiting our website, you acknowledge that your personal information may be processed in accordance with this Privacy Notice.

---

2. Data Controller

M4 Digital Group Ltd is the Data Controller responsible for the personal information described in this Privacy Notice.

M4 Digital Group Ltd

Temple Court, 13a Cathedral Road, Cardiff, CF11 9HA

Telephone: +44 (0)2920 647647
Website: www.m4digitalgroup.com
Email: info@m4digitalgroup.com

For all privacy-related enquiries and requests to exercise your data protection rights, please contact:

Data Protection Lead
Email: info@m4digitalgroup.com

---

3. Personal Information We Collect

Depending on your relationship with us, we may collect and process the following categories of personal information.

Identity Information

- Full name
- Title
- Date of birth (where required)
- Nationality (where required)

Contact Information

- Home address
- Business address
- Telephone numbers
- Email addresses

Professional Information

- Employment history
- CVs and résumés
- Qualifications and certifications
- Security clearances
- Professional memberships
- References

Financial Information

- Bank account details
- Tax information
- Payment and invoicing information

Technical Information

When you use our website or systems, we may collect:

- IP address
- Browser type and version
- Device information
- Operating system information
- Website usage data
- Cookie preferences

Special Category Data

In limited circumstances, and only where legally permitted, we may process:

- Health information
- Equality, diversity and inclusion information
- Criminal conviction information
- Security vetting information

Where Special Category Data is processed, M4 will do so only where an appropriate condition under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018 applies.

---

4. How We Collect Information

We may collect personal information:

- Directly from you
- Through recruitment processes
- Through contracts and commercial engagements
- Through correspondence and communications
- Through our website
- From recruitment agencies and screening organisations
- From customer organisations where appropriate
- From publicly available professional sources
- From referees nominated by you

---

5. Website Visitors, Analytics and Cookies

Our website may use cookies and similar technologies to improve security, functionality and user experience.

Where legally required, we will obtain your consent before placing non-essential cookies on your device.

Website analytics may be used to help us understand how visitors interact with our website and identify opportunities for improvement.

Where permitted by applicable legislation, certain cookies or similar technologies may be used without consent where they are strictly necessary, security-related, or otherwise exempt under privacy regulations. Information regarding such technologies will be provided through our Cookie Policy and website privacy controls.

Further information is available in our Cookie Policy.

---

6. Lawful Bases for Processing

We process personal information only where permitted under applicable data protection legislation.

The lawful bases relied upon may include:

Contract

Processing necessary for:

- Entering into a contract
- Delivering services
- Managing supplier relationships
- Managing contractor engagements

Legal Obligation

Processing necessary to comply with:

- Employment legislation
- Tax legislation
- Immigration legislation
- Regulatory requirements
- Security requirements

Legitimate Interests

Processing necessary for legitimate business purposes, including:

- Recruitment
- Workforce planning
- Business administration
- Information security
- Service delivery
- Business development
- Contract management

Consent

Where consent is relied upon, you may withdraw that consent at any time.

---

7. Recruitment and Contractor Applications

When you apply for employment, consultancy or contract opportunities with M4, we process personal information for the purposes of:

- Assessing suitability for roles
- Managing recruitment activities
- Verifying qualifications and experience
- Conducting pre-employment checks
- Communicating regarding opportunities
- Meeting customer, legal and regulatory requirements

Information requested may include:

- CVs and employment history
- Proof of identity
- Proof of address
- Qualifications and certifications
- Right-to-work documentation
- References
- Security screening information

We will only collect information that is relevant and proportionate for the intended purpose.

Recruitment Talent Pool

Where appropriate and with your consent, we may retain recruitment records, CVs and contact information for up to 12 months following an application in order to contact you regarding future employment, consultancy or contract opportunities.

You may withdraw your consent at any time.

---

8. Referees and Emergency Contacts

M4 may process personal information relating to referees and emergency contacts supplied by candidates, employees, contractors or consultants.

Such information will only be used for:

- Employment verification
- Reference checking
- Emergency contact purposes
- Compliance with customer or contractual requirements

The information will be retained only for as long as required for these legitimate purposes.

---

9. Baseline Personnel Security Standard (BPSS)

Where required by customer, contractual or regulatory obligations, M4 Digital Group Ltd may undertake Baseline Personnel Security Standard (BPSS) screening.

BPSS screening may include verification of:

- Identity
- Nationality and immigration status
- Right to work in the United Kingdom
- Employment history
- Unspent criminal convictions
- Qualifications and professional credentials

Information collected as part of BPSS screening will only be used for recruitment, onboarding, security assurance and compliance purposes.

Where appropriate, screening may be conducted by approved third-party screening providers acting under contractual obligations to protect your information.

---

10. Security Clearance and Government Client Requirements

M4 Digital Group Ltd delivers services to customers operating within government, defence, critical national infrastructure and other regulated sectors.

Where required by customers, contracts or statutory obligations, we may process personal information relating to security vetting and personnel assurance activities.

This may include information relating to:

- Baseline Personnel Security Standard (BPSS)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Developed Vetting (DV)
- Other government-approved vetting levels

Personal information may be processed to:

- Verify existing clearances
- Support client onboarding requirements
- Sponsor clearance applications
- Maintain records of clearance status
- Meet contractual security obligations
- Facilitate access to secure systems, sites and information

Certain assignments may require compliance with customer-specific security, information assurance or personnel assurance requirements. Personal information may be shared with authorised customer organisations, government departments, vetting authorities or approved screening providers where necessary to fulfil contractual, legal or security obligations.

Decisions regarding the granting, suspension, review or withdrawal of security clearances are made by the relevant government authority and not by M4 Digital Group Ltd.

Access to security-related information is restricted to authorised personnel with a legitimate business need.

Security clearance information will be retained only for as long as required to satisfy customer, contractual, legal, regulatory or security obligations.

---

11. Who We Share Information With

We may share personal information with:

- Customers and prospective customers where necessary
- Professional advisers
- Recruitment partners
- Payroll providers
- Benefits providers
- IT service providers
- Cloud hosting providers
- Security screening suppliers
- Government and regulatory bodies
- Law enforcement agencies where legally required

We do not sell personal information to third parties.

Where third-party processors act on our behalf, they are contractually required to process personal information only in accordance with our instructions and applicable data protection legislation.

---

12. International Transfers

Some of our suppliers and service providers may process personal information outside the United Kingdom.

Where international transfers occur, we ensure that appropriate safeguards are implemented in accordance with UK data protection legislation, including:

- UK adequacy regulations
- International Data Transfer Agreements (IDTAs)
- UK Addendum to Standard Contractual Clauses
- UK-US Data Bridge arrangements, where applicable

- Other recognised transfer mechanisms

---

13. Data Security

We maintain appropriate technical and organisational measures designed to protect personal information against:

- Unauthorised access
- Accidental loss
- Misuse
- Unlawful disclosure
- Destruction or damage

Security measures include access controls, staff training, contractual controls and information security policies appropriate to the nature of our business and customer requirements.

If you become aware of any suspected misuse, loss or unauthorised access involving your personal information, please notify M4 Digital Group Ltd immediately using the contact details provided in this notice.

---

14. Data Retention

We retain personal information only for as long as necessary for the purposes for which it was collected and to satisfy legal, regulatory and contractual obligations.

Record Type	Retention Period
Recruitment records (unsuccessful applicants)	Up to 12 months
Customer and supplier records	6 years after relationship ends
Financial records	6 years
Employee records	In accordance with statutory requirements
Security and vetting records	As required by customer, contractual, regulatory or security obligations

Retention periods may be extended where necessary:

- To establish, exercise or defend legal claims
- To support audits or investigations
- To comply with legal or regulatory requirements

---

15. Your Rights

Under UK GDPR, you have the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making
- Right to withdraw consent where applicable

---

16. Subject Access Requests

You may request access to the personal information we hold about you at any time.

Requests should be submitted to:

info@m4digitalgroup.com

We will respond without undue delay and normally within one calendar month unless an extension is permitted by law.

Where permitted by applicable legislation, M4 Digital Group Ltd may seek clarification regarding a request where additional information is required to identify the information requested. In such circumstances, statutory response periods may be paused in accordance with applicable legal requirements.

---

17. Automated Decision-Making

M4 Digital Group Ltd does not routinely carry out solely automated decision-making that produces legal or similarly significant effects on individuals.

Where automated decision-making is used in the future, M4 Digital Group Ltd will implement appropriate safeguards in accordance with applicable data protection legislation.

These safeguards may include:

- Providing information about significant automated decisions;
- Enabling individuals to request meaningful human intervention;
- Allowing individuals to express their views regarding a decision; and
- Providing individuals with the opportunity to challenge a decision where applicable.

---

18. Data Protection Complaints

M4 Digital Group Ltd is committed to handling privacy and data protection concerns fairly, transparently and without undue delay. Requirements relating to organisational complaints handling were introduced under the Data (Use and Access) Act 2025.

If you have concerns regarding how your personal information has been collected, used, stored or disclosed, you may submit a complaint using the contact details provided within this Privacy Notice.

Complaints should be submitted to:

Data Protection Lead
Email: info@m4digitalgroup.com

M4 Digital Group Ltd will acknowledge, investigate and respond to complaints in accordance with applicable data protection legislation and internal procedures.

---

19. Complaints and Regulatory Oversight

If you remain dissatisfied following our response to a privacy or data protection complaint, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

We would, however, appreciate the opportunity to address your concerns before you approach the ICO where possible.

Information Commissioner's Office (ICO)

Website: www.ico.org.uk
Telephone: 0303 123 1113

The ICO is the UK's independent authority responsible for upholding information rights and enforcing data protection legislation.

---

20. Changes to this Privacy Notice

We review this Privacy Notice regularly and may update it from time to time to reflect changes in legislation, regulatory guidance, technology or business practices.

The most current version will be made available upon request and through appropriate company communication channels.

This policy was last updated November 2026