GRC+

Privacy Notice

CLASSIFICATION	VERSION	IN EFFECT FROM
PUBLIC	3.2	14 March 2026

LATEST VERSION
grc.plus/privacy

Check this address before you rely on a printed or saved copy.

© 2026 GRC+

Document Control

FIELD	VALUE
Classification	PUBLIC: may be shared with anyone
Version	3.2
In effect from	14 March 2026
Latest version	grc.plus/privacy

© 2026 GRC+

Contents

1	Who we are	4
2	When we use your data as a processor	4
3	What we use and why	5
4	Where your data comes from	15
5	Microsoft Teams and other platforms	15
6	Who we share data with	15
7	Transfers outside Europe	16
8	How we protect your data	16
9	Your rights	17
10	Automated decisions and AI	18
11	Complaints	18
12	Children	18
13	Changes to this notice	19
14	Contact	19

© 2026 GRC+

This notice explains what personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. GRC+ uses, why, on what legal basis, how long we keep it and what rights you have. It applies when you visit our website, contact us, work with us as a client or supplier, attend our training or events, apply for a job, or use a GRC+ app or bot in Microsoft Teams or another platform. It is written to meet Articles 13 and 14 of the General Data Protection RegulationAn EU regulation governing the processing of personal data and the free movement of that data. It establishes data protection principles, rights for individuals and obligations for controllers and processors. (GDPRGeneral Data Protection Regulation) and the UK GDPRUnited Kingdom General Data Protection Regulation.

1 Who we are

The controllerThe person, public authority, agency or other body that, alone or jointly with others, decides the purposes and means of processing personal data. The controller carries primary responsibility for GDPR compliance and must be able to demonstrate it. of your personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. is **GRC PLUS B.V.** (trading as GRC+), a private limited company registered with the Netherlands Chamber of Commerce under number 83892648, with its corporate seat in Amsterdam, the Netherlands.

Our UK company, GRC PLUS LTD (company number 13664716, England and Wales), is part of the same group. Where it is involved in your relationship with us, it uses your data in the same way and under this notice.

For any question about this notice or your data, write to privacy@grc.plus. We have not appointed a Data Protection OfficerA person with expert knowledge of data protection law who assists a controller or processor in complying with the GDPR. Article 37 of the GDPR sets out when designating a DPO is mandatory.: the GDPRGeneral Data Protection Regulation does not require one for our activities. A named senior person at GRC+ is responsible for privacy and answers every request.

2 When we use your data as a processor

When a client asks us to handle personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. for them, for example as their outsourced DPOData

Protection Officer, during an audit or when we review their supplier contracts, the client decides how that data is used. We then act as a processorA person, public authority, agency or other body that processes personal data on behalf of a controller. The processing must be governed by a contract or another binding legal act under Union or Member State law meeting GDPR Article 28(3), and the processor must follow the applicable documented-instruction requirements. under a data processing agreementA contract setting out how a processor handles personal data on a controller's behalf. Under GDPR Article 28(3), the processing must be governed by a contract or another binding legal act with specified terms., and the client's own privacy notice applies. If you have a question about such data, contact that organisation first; we will help them answer you.

3 What we use and why

The table lists each purpose, the data involved, the legal basis under Article 6 GDPRGeneral Data Protection Regulation and how long we keep it.

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Answering questions, quote requests and messages sent through our forms, by e-mail or phone	Name, work e-mail, company, phone number, your message, the page you sent it from	Steps you asked for before a contract (6(1)(b)); our legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in answering business enquiries (6(1)(f))	12 months after our last contact, unless you become a client
Booking a meeting with us	Name, e-mail, company, what you want to discuss, the time you choose	6(1)(b) and 6(1)(f), as above	12 months after the meeting, unless you become a client

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Online meetings (Microsoft Teams and similar)	Name, e-mail, what you say and show during the call, chat messages; a recording or transcript only when we announce it at the start	Legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in holding the meeting (6(1)(f)); for recordings, your agreement at the start of the call	Recordings and transcripts: deleted within 90 days, unless they form part of a deliverable you asked for
Delivering services to clients, managing the engagement, invoicing	Names, roles and contact details of client staff, contract and billing details, correspondence, work papers	Performance of our contract (6(1)(b)); legal obligations such as tax law (6(1)(c))	For the duration of the contract, then 7 years for financial records (Dutch tax law); audit and assessment files as long as professional standards require, usually 7 years

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Online sign-up and subscription payments	Name, e-mail, company, billing address, VAT number, chosen plan and add-ons, payment status. Card or bank details are entered on Stripe's pages; we never see full card numbers.	6(1)(b) and 6(1)(c)	For the subscription, then 7 years for financial records
Training, courses and events	Name, e-mail, company, job title, attendance, exam results and certificates, dietary needs if you tell us	6(1)(b); for dietary needs that reveal health or religion, your explicit consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard. (9(2)(a))	Invoices 7 years; attendance and certificates 5 years so we can confirm them; dietary needs deleted after the event

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Contacting business professionals about services relevant to their role	Name, job title, employer, work e-mail and phone, LinkedIn profile, taken from public sources such as company websites, LinkedIn and tender notices	Our legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in business development (6(1)(f)). You can object at any time and we will stop.	Reviewed every 24 months; deleted when no longer relevant. If you object, we keep only what is needed to respect that.

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Newsletters and updates	Name, e-mail, topics you choose, whether you open or click our e-mails	Your consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard. (6(1)(a)); for existing clients, our legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in sending updates about similar services (6(1)(f)), as Dutch law allows	Until you unsubscribe; every e-mail has an unsubscribe link

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Website analytics and advertising measurement	Pages visited, clicks, device and browser type, approximate location, a cookieA small text file that a website saves on a computer or mobile device. It lets the site remember information between pages or visits, such as a login, language choice or other preference. Cookies can support a site's functions or provide information about its use. The term identifies the storage technology; whether a particular cookie needs consent depends on its purpose and the law that applies. identifier	Your consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard. via the cookieA small text file that a website saves on a computer or mobile device. It lets the site remember information between pages or visits, such as a login, language choice or other preference. Cookies can support a site's functions or provide information about its use. The term identifies the storage technology; whether a particular cookie needs consent depends on its purpose and the law that applies. bar (6(1)(a))	As set out in our cookie policy; Google Analytics data at most 14 months

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Running and protecting the website	IP addressInternet Protocol Address, browser, pages requested, time, error logs; the country your IP addressInternet Protocol Address belongs to, to show local phone numbers and content; when you use one of our forms, the Cloudflare Turnstile check, which looks at your IP addressInternet Protocol Address and browser signals to tell people from automated spam	Legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in a secure, working website (6(1)(f))	Server and security logs up to 90 days; the country choice is stored in your browser only; Cloudflare keeps the Turnstile check’s data under its own privacy terms

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Job applications	CV, contact details, motivation, LinkedIn profile, interview notes, work sample, references (only with your permission). Applications come in through the form on the job page: the CV is stored encrypted on our website server and only the hiring team can open it. We never ask you to e-mail a CV. Your name, e-mail and the role are also recorded in our CRMCustomer Relationship Management (HubSpot, EU data centre) as a candidate, separate from client records.	Steps you asked for before a contract (6(1)(b)) and our legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. in recruiting (6(1)(f))	Deleted automatically 4 weeks after the role closes, and never later than 6 months after you applied; 1 year if you agree we may keep your application for other roles
Working with suppliers and partners	Contact details, contract and payment details, correspondence	6(1)(b) and 6(1)(f)	Contract term plus 7 years for financial records

© 2026 GRC+

PURPOSE	PERSONAL DATAANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON, THE DATA SUBJECT. A PERSON IS IDENTIFIABLE IF THEY CAN BE IDENTIFIED DIRECTLY OR INDIRECTLY, FOR EXAMPLE BY A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR FACTORS SPECIFIC TO THEIR IDENTITY.	LEGAL BASIS	HOW LONG
Handling complaints, privacy requests and security reports	What you send us and our replies	Legal obligation (6(1)(c)) for privacy requests; legitimate interestA basis under the EU General Data Protection Regulation (GDPR) for using personal data when this is necessary to pursue a legitimate interest of the organisation deciding why and how the data is used, or of a third party. This basis cannot be used if the affected person's interests or fundamental rights and freedoms override that interest, with particular care needed for children. Business benefit alone does not establish permission. Public authorities cannot use this basis when performing their official tasks. (6(1)(f)) for the rest	2 years after the matter is closed
Meeting legal obligations and defending legal claims	What the obligation or claim requires	6(1)(c) and 6(1)(f)	As long as the obligation or the claim lasts

Where we rely on legitimate interestsLegitimate Interest, we have weighed them against your interests and rights. You can ask us for that assessment.

4 Where your data comes from

Mostly from you: through our forms, e-mail, calls, meetings and applications. We also receive data from your employer when you are a contact at a client, supplier or partner; from people who refer you to us; from Stripe and HubSpot when you sign up or book a meeting; and, for business development, from public professional sources such as company websites, LinkedIn and public tender notices.

5 Microsoft Teams and other platforms

If you meet with us on Microsoft Teams, Microsoft processes the call under its own terms, and our tenant is set up in Microsoft's EU Data Boundary where Microsoft offers it. If you use a GRC+ app, connector or bot in Microsoft Teams or another platform, we process what is needed to run it: your name, e-mail address, organisation and tenant identifier, and the messages or files you send to it. We use that content only to provide the function you asked for. We do not use it to train AIArtificial Intelligence models, we do not sell it, and we delete it when you remove the app or when the related engagement ends, unless the law requires us to keep it.

6 Who we share data with

We do not sell personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity., and we share it only when needed for the purposes above:

- **Service providers who process data for us**, such as our e-mail and office software, CRMCustomer Relationship Management, website host and payment provider. They work under data processing agreementsData Processing Agreement and only on our instructions. The current list is on our sub-processors page.
- **Associates and partners** who work on an engagement with us, under confidentialityThe information-security property of keeping information from being disclosed to people, organisations or systems that are not authorised to receive it. Access restrictions and encryption help preserve confidentiality when information is stored, sent or processed. It concerns who can see information; it does not by itself ensure that the information is accurate or that a service remains available. terms, and only after the client has agreed to their involvement.
- **Professional advisers** such as our accountant, auditors, lawyers and insurers, who are bound by professional secrecy or contract.
- **Authorities** such as the tax authority or a court, when the law requires it.

© 2026 GRC+

- **Analytics and advertising platforms** (Google, Microsoft, LinkedIn, HubSpot), only after you accept those cookiesCookie. For the data their tags collect on our site, we and the platform can be joint controllersThe person, public authority, agency or other body that, alone or jointly with others, decides the purposes and means of processing personal data. The controller carries primary responsibility for GDPR compliance and must be able to demonstrate it.; you can ask us for the essence of those arrangements.

7 Transfers outside Europe

We choose providers that keep data in the European Economic AreaThe area created by the EEA Agreement, which brings together the EU Member States and Iceland, Liechtenstein and Norway in the internal market. EU laws marked as having EEA relevance, such as the GDPR, can extend to those three countries. where they can, for example HubSpot's EU data centre and Microsoft's EU Data Boundary. Some providers or their support teams are in the United States or other countries. Such transfers take place only with a safeguard the GDPRGeneral Data Protection Regulation recognises: an adequacy decisionAdequacy Decision (EU GDPR) (including the EU-US Data Privacy FrameworkA framework for transferring personal data from the European Economic Area to participating organisations in the United States. US organisations self-certify that they follow its privacy principles, and the European Commission's adequacy decision recognises protection for covered transfers. Businesses must check that the particular recipient and relevant data are covered by an active certification. A US location alone does not establish eligibility. for certified companies), or the European Commission's Standard Contractual ClausesModel data protection clauses adopted by the European Commission that provide appropriate safeguards for transfers of personal data to countries outside the EEA. Organisations use them in contracts with recipients outside the EEA. with additional measures where needed. Transfers between our Dutch and UK companies rely on the adequacy decisions the EU and the UK have adopted for each other. You can ask for a copy of the safeguard that applies.

8 How we protect your data

We work in information securityProtecting information and the systems that handle it so that only authorised people can access it, it remains accurate and complete, and it is available when needed. These aims are called confidentiality, integrity and availability. Information security combines organisational requirements, staff practices and technical safeguards to reduce risks such as disclosure, alteration, disruption or destruction. and hold ourselves to what we recommend to clients. Measures include multi-factor authenticationAuthentication through verification of at least two different types of factor: something a person knows, such as a password; something they have, such as a token; or something they are, such as a biometric. NIS2, PCI DSS, the NYDFS regulation and the FTC Safeguards Rule call for it. on every account,

encryptionEncryption changes readable information into an unreadable form using a mathematical method and a key, a value that controls the transformation. Decryption recovers the original information with the appropriate key. Encryption helps keep stored or transmitted data confidential, so people without the necessary key cannot readily read it. of data in transit and at rest, managed and encrypted devices, access limited to the people who need it, logging, regular updates, careful selection of suppliers, and confidentialityThe information-security property of keeping information from being disclosed to people, organisations or systems that are not authorised to receive it. Access restrictions and encryption help preserve confidentiality when information is stored, sent or processed. It concerns who can see information; it does not by itself ensure that the information is accurate or that a service remains available. obligations for everyone who works with us. If a personal data breachA breach of security leading to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data. A controller must notify the supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless it is unlikely to result in a risk to people's rights and freedoms. happens, we follow our incident procedure: we notify the Dutch Data Protection AuthorityAn independent public body that supervises compliance with data protection law. Under the GDPR, such authorities monitor and enforce its application, handle complaints and exercise investigative and corrective powers. within 72 hours where required, and we tell you without delay if the breach is likely to put you at high risk.

9 Your rights

You have the right to:

- ask for a copy of the personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. we hold about you (access);
- have incorrect data corrected and incomplete data completed;
- have data deleted, for example when we no longer need it or you withdraw consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard.;
- ask us to restrict use of your data while a question about it is being resolved;
- receive data you gave us in a common machine-readable format, or have it sent to another organisation (portability);
- object to our use of your data based on legitimate interestsLegitimate Interest. You can always object to direct marketing, and we will then stop without asking for a reason;
- withdraw consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal

data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard. at any time, without affecting what we did before. For cookiesCookie, use the cookie settings.

Send your request to privacy@grc.plus. It is free. We answer within one month; for complex requests we may extend this by up to two months and will tell you why. To protect your data we may ask you to confirm your identity, but we will not ask for more than we need, and never for a copy of your passport.

10 Automated decisions and AI

We do not make decisions about you based solely on automated processing, including profilingAny automated processing of personal data that evaluates personal aspects of a person, in particular to analyse or predict their work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movements. The GDPR, AI Act, DSA and DMA all attach specific requirements to it., that have legal or similarly significant effects. We use AIArtificial Intelligence tools to help draft and analyse, always with human review, under the safeguards in our responsible AI statement. We do not put client confidential data or your application documents into AIArtificial Intelligence tools that may use them for training.

11 Complaints

If you are unhappy with how we use your data, please tell us first at privacy@grc.plus; most issues are solved quickly. You also have the right to complain to a data protection authorityAn independent public body that supervises compliance with data protection law. Under the GDPR, such authorities monitor and enforce its application, handle complaints and exercise investigative and corrective powers.. In the Netherlands this is the Autoriteit PersoonsgegevensAutoriteit Persoonsgegevens (Dutch Data Protection Authority) (autoriteitpersoonsgegevens.nl). In the United Kingdom it is the Information Commissioner's Office (ico.org.uk). You can also complain to the authority in the EU country where you live or work.

12 Children

Our services and website are meant for organisations and professionals. We do not knowingly collect data from children under 16. If you think we have, write to us and we will delete it.

© 2026 GRC+

13 Changes to this notice

We update this notice when our processing changes or the law requires it. The version and date are at the top of the page. For significant changes that affect clients or subscribers, we will also tell you by e-mail.

VERSION	DATE	CHANGE
2.1	19 October 2026	Job applications: encrypted storage and automatic deletion, candidate record in our CRMCustomer Relationship Management. Separate addresses for privacy (privacy@grc.plus) and legal matters (legal@grc.plus).
2.0	19 October 2026	Rewritten in full: table of purposes, legal bases and retention; job applicants, online meetings, Teams apps, online sign-up, business development and international transfers added.
1.0	18 February 2026	Earlier notice focused on cookiesCookie and consentA freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data. The ePrivacy Directive, the DMA and the DGA rely on the same GDPR standard..

14 Contact

GRC PLUS B.V. · Keurenplein 41, 1069 CD Amsterdam, Netherlands · Chamber of Commerce 83892648
Privacy questions and requests: privacy@grc.plus

Is this the latest version?
Scan the code or open grc.plus/privacy. Version 3.2 was in effect from 14 March 2026.

This PDF is saved as PDF/A-1b for archiving. © 2026 GRC+

END OF DOCUMENT