



RECRUITMENT PRIVACY NOTICE

AUGUST 2026

avis budget group

Contents

<u>ABG AMERICAS & INTERNATIONAL PRIVACY POLICY</u>	<u>1</u>
<u>COOKIE NOTICE</u>	<u>9</u>
<u>APPENDIX A</u>	<u>12</u>
<u>APPENDIX B</u>	<u>13</u>



ABG AMERICAS & INTERNATIONAL PRIVACY POLICY

1 Contact details

This privacy notice applies to personal information collected by Avis Budget Group including Avis Car Sales and Zipcar (“ABG”/“we”/“us”/“our”) in connection with a job application submitted by you or otherwise during the recruitment process.

Our Privacy Office for the Americas can be contacted via ABGprivacy@avisbudget.com or by post at Avis Budget Group, 6 Sylvan Way, Parsippany, NJ 07054 Attn: Privacy Office.

Our Privacy Office for the EMEA region can be contacted via DPO@abg.com or by post at Avis Budget House, Park Road, Bracknell, Berkshire, RG12 2EW, England, UK.

Our Data Privacy Representative for India is Sandya GR who can be contacted via Sandya.GR@avisbudget.com or by post at Roshini Tech Hub, PFS Club House, Marathahalli Main Road, Lakshminarayana Pura, Epip Zone, Chinnapanna Halli, Bengaluru, Karnataka 560037. Sandya can also be contacted on the Global Integrity Hotline at 000-800-040-1302.

Where you are applying for a role with one of our companies in the European Economic Area, that company will be the “data controller” of the personal information collected about you. Details of the relevant company as well as its contact details, are available in the job description or by speaking to your local HR team (being the ABG HR team that you speak to in relation to your application).

This privacy notice should be read in conjunction with the Avis privacy notice available to you on your local ABG website, which also includes details of how you can make privacy-related complaints under applicable law and how we will deal with those complaints.

2 Personal Information Collected

We collect the information set out at **Appendix A** about you during the recruitment process when you apply for a role. If you fail to provide certain information when requested, we will not be able to progress your application.



3 How we use personal information

- 3.1** We use your personal information to: (a) contact you during your candidacy for employment, send you announcements, request additional information as required, and otherwise progress the recruitment process; (b) assess and make a decision about your suitability for a role. This may include initial questions in relation to key skills or requirements needed for a specific role. If you do not have these key skills or meet these requirements, you may not be able to proceed with the application. If you have any queries in relation to these questions, please contact talent.acquisition@avisbudget.com; (c) to communicate with you, including to offer you the role in cases where we decide to do so; (d) to carry out reference or background checks and verify your eligibility for a role after an offer of employment is made.
- 3.2** We will also use your information to comply with legal and regulatory requirements and to comply with our contractual obligations to our customers (to the extent permitted by applicable law). For example, complying with duties under employment, social security, social protection and tax legislation, as well as to meet our government reporting requirements.

4 Sources of Information

This information is either: (a) provided by you to us, including information you provide through automated recruitment systems that we use during the course of or in connection with the recruitment process; (b) obtained from third parties through the application and recruitment process including from credit reference agencies; (c) obtained from recruitment agencies, research providers or third party job platforms; (d) obtained from previous employers who you have included as references; or (e) created by us in the course of the recruitment process.



We may use automated employment decision-making technologies as one tool in the recruiting process for certain roles. These technologies are not meant to replace decision-making by our recruiters but rather assist with the assessment or evaluation of such candidates. As part of our hiring process, you may be asked to complete one or more assessments. One focuses on your personality — it's designed to gauge your personality, interests, and work-related attitudes, which helps us evaluate how well you align with the aptitudes we look for in successful employees. A second assessment evaluates cognitive ability. This matters because our work environment is challenging, fast-paced, and requires people who can keep learning and adapting over time. Our technology partner has conducted bias audits of this technology. Please visit their website for more details: <https://www.traitify.com/ethical-assessments>.

5 Why we use personal information

We will use the information for the purposes for which you have provided consent. In particular, we will use the information collected from you because: (a) it is necessary for us to do so before entering into an employment relationship with you; (b) we need to process your information in order to comply with a legal or regulatory obligation; (c) to ensure the effective administration and management of the recruitment process; (d) to help us ensure we hire a suitable individual for a role; (e) to deal with disputes and accidents and take legal action or obtain legal or other professional advice; and (f) to ascertain your fitness to work.

6 How we use special category personal information

We will process your special categories of personal data: (a) to consider whether we need to provide appropriate adjustments during the recruitment process and to ascertain your fitness to work; (b) for equal opportunity monitoring purposes; or (c) to comply with any legal or regulatory obligation. Details of the special categories of personal data we process are contained in **Appendix A**.



7 Why we use special category personal information

We will use special categories of personal information collected about you because: (a) you have voluntarily elected to provide such information when requested for our monitoring, compliance, and government reporting purposes; (b) we need to do so to carry out our legal obligations; (c) it is necessary for the establishment, exercise, or defense of legal claims on in relation to court cases; and/or (d) there is a substantial public interest.

8 Verifying eligibility for a role

Your eligibility for a role will be verified after an offer of employment is made. We will provide you with further information in relation to this verification and, if required by applicable law, request your consent to such verification, after an offer of employment is made.

As part of the recruitment process, we may use a third-party vendor to work with you to obtain information in relation to unspent criminal convictions and we may carry out criminal background checks subject to the respectively applicable labour and privacy laws. We will notify you in the course of your application if these checks will be carried out in respect of the role you are applying for. We use this information and these checks: (a) to assess your suitability for a regulated role; (b) to protect your interests, our interests, and third-party interests; and/or (c) where it is necessary in relation to legal claims. We are allowed to use your personal information in this way where applicable law allows it and where it is necessary to carry out our employment rights and obligations; you have given your consent; or it is needed to prevent any unlawful act from potentially occurring and this must be carried out without your consent.

9 Information that we share

We will only share your personal information with the following third parties for the purposes of processing your application: (a) employment agencies; (b) background check and online test providers; (c) credit reference agencies; (d) regulators and authorities; (e) third party IT service providers such as our HR system provider or companies that develop and operate automated recruitment systems that we use during the course of or in connection with the recruitment process; and (g) previous employers for the purposes of reference checking. We will also share personal data within the ABG group for the purposes of administration, accounting, and reporting purposes.



10 Security and Retention of your information

We use reasonable physical, administrative, and organizational measures to protect your information from unauthorized use, access, disclosure, alteration, destruction, or loss. Further, we impose various security requirements on our third-party service providers who may process personal information on our behalf.

We will retain your personal information for the duration of the recruitment process and for the length required to comply with any applicable local legal requirements. If you are successful in applying for a position, your personal information will be retained for a further period in connection with your employment and in accordance with our Record and Information Management Policy. This will be as set out within our Employee Privacy Notice which will be made available to you on employment.

11 Where your information will be held

11.1 Your personal information may be transferred and / or stored outside your country of residence and subject to laws of that jurisdiction, including:

11.1.1 **If applying from outside the EMEA region** to companies within the ABG group located in one of the European Economic Area member states or in the UK, Switzerland, or to countries where the European Commission determined there is an adequate level of data protection of the Employee Data;

11.1.2 **[if applying within the European Economic Area]** to ABG group companies located outside the European Economic Area including the United States of America such as Avis Budget Group, Inc. and, following the date upon which it ceases to be a member state of the European Union, the United Kingdom based on the conclusion of a model contract in accordance with the decision of the European Commission No. 2004/915/EC; and

11.1.3 to ABG group companies located in the United States of America, Canada and other countries where ABG operates; and



- 11.1.3 to ABG group companies located in the United States of America, Canada, and other countries where ABG operates; and
- 11.1.4 to third party IT service providers located both within the European Economic Area member states or in Switzerland or to countries where the adequate protection of the Employee Data is ensured and outside the European Economic Area based on the conclusion of a model contract in accordance with the decision of the European Commission No. 2004/915/EC.
- 11.1.5 You can view copies of the model clauses at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

12 Your rights

- 12.1 Where available under local applicable privacy law, you may have certain rights over your information, and we've explained below how you can use these rights if applicable under local law. These rights are subject to certain exemptions.

Where available under local applicable privacy law you may have certain rights over your information if you are a resident in the European Economic Area or are applying for a role with one of our companies located in the European Economic Area. For applicants in the EMEA region, the following rights are applicable under the General Data Protection Regulations (GDPR):

- 12.1.1 **Right of access:** you may have the right to request access to the personal information we have about you and to request supporting information explaining how the personal information is used.
- 12.1.3 **Right of rectification:** you may have the right to request that we rectify inaccurate personal information about you.
- 12.1.4 **Right to erasure ('right to be forgotten')**: you may have the right to request that we delete your personal information, subject to certain exceptions under applicable law.



- 12.1.5 Right to restrict processing:** in some situations, you may have the right to request that we do not use the personal information you have provided (e.g. if you believe it to be inaccurate).
- 12.1.6 Right to data portability:** you may have the right to receive certain of your personal information in a structured, commonly used, and machine-readable format and to transmit such information to another controller.
- 12.1.7 Right to withdraw consent:** where we process your personal information based on consent, you have the right to withdraw consent at any time. However, this will not affect the lawfulness of the processing based on consent before its withdrawal. Furthermore, even in case of a withdrawal, we may continue to use your personal information as permitted or required by law.
- 12.1.7 Right to object:** where we are processing your personal information based on a legitimate interest (or those of a third party) you may challenge this. However, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to legal claims.
- 12.1.8** In addition, if specifically provided for under your local law, you will have a right to define post-mortem guidelines – meaning you may define guidelines regarding the storage, erasure, and disclosure of your personal data after your death. And you may have further rights to access the personal information that we hold about you and request the correction of any of your personal information. Further details of such rights are contained on the Avis privacy notice available to you on your local Avis website.
- 12.1.9** Please get in touch with our Data Protection Officer at DPO@abg.com if you would like to exercise any of these rights or in case you should have any concerns about how we process your personal information. You are also free to lodge a complaint with the supervisory authority or regulatory body, should you feel that we process your personal information in a way that is against applicable law. Further details of your local supervisory authority or regulatory body can be found at Appendix B.

We will ask you to verify your identity before carrying out a request.



12.2 For applicants primarily based in California, rights under the California Consumer Privacy Act (CCPA) can be exercised as follows:

12.2.1 Right to Know: You can request information about what personal data a company has collected about you, how it's being used, and whether it's being shared or sold.

12.2.2 Right to Access: You can request a copy of the specific personal information a company has collected about you in the past 12 months.

12.2.3 Right to Delete: You can request that a company delete your personal information, with some exceptions.

12.2.4 Right to Opt-Out: You can tell businesses not to sell your personal information. However, this is less relevant for job applicants as companies typically don't sell applicant data.

12.2.5 Right to Non-Discrimination: Companies cannot discriminate against you for exercising your CCPA rights.

12.2.6 Right to Correct: You can request that inaccurate personal information be corrected.

12.3 To exercise an applicable right, or in case you should have any concerns about how we process your personal information, please fill out our form by clicking here: [Data Subject Rights Request Form](#) or get in touch with us at ABGprivacy@avisbudget.com (for North America residents) and DPO@abg.com (for International residents).

12.3.1 We will ask you to verify your identity before carrying out a request.

12.4 We do not share your personal information with third parties for their own direct marketing purposes.

13 Minors & Children

13.1 This website is not for children under the age of 16. We do not knowingly collect personal information from children. If you think we have received personal information from children under the age of 16, please contact us immediately.



COOKIE NOTICE

This Notice describes how we use cookies and similar technologies on our website and mobile apps.

Last updated in July 2024.

We use cookies and similar technologies as described in this Notice. Where you have consented to our use of cookies, you agree that we can distinguish you from other users of our website and apps for the purposes set out below. This helps provide you with good user experience, tailored content, and interest-based adverts. For example, we can recognize and remember important information that will make it more comfortable for you to browse our website or use our apps such as preferred settings. It also helps us to detect and prevent fraud.

What are cookies and similar technologies?

A cookie is a small file of letters and numbers that we store via your browser on the hard drive of your computer or mobile device.

There are three main types of cookies:

- **Session cookies:** specific to a particular visit and limited to sending session identifiers (random numbers generated by the server) so you don't have to re-enter information when you navigate to a new page or check out. Session cookies are not permanently stored on your device and are deleted when the browser closes.
- **Persistent cookies:** record information about your preferences and are stored in your browser cache or mobile device.
- **Third party cookies:** placed by someone other than us which may gather data across multiple websites or sessions.



We use cookies for the following purposes:

Type of Cookie	Purpose of Cookie
Strictly necessary	These cookies are essential for you to browse our website and use its features. The information collected relates to the operation of the Website (e.g. website scripting language and security tokens) and enables us to provide you with the service you have requested.
Functionality	These cookies remember the choices you have made, for example the country you visit our Website from, your language and any changes you have made to text size and other parts of the web pages that you can customise to improve your user experience and to make your visits more tailored and enjoyable. The information these cookies collect cannot be used to track your browsing activity on other websites.
Performance/analytics	These cookies collect information on how users use our Website, for example which pages you visit most often, whether you receive any error messages, and how you arrived at our website. Information collected by these cookies is used only to improve your use of our Website. These cookies are sometimes placed by third party providers of web traffic and analysis services. We use Google Analytics. For information on how Google processes and collects your information and how you can opt out, please see the following link: https://tools.google.com/dlpage/gaoptout .
Targeting or advertising	These cookies collect information about your browsing habits and inferred interests to make advertising more relevant to you. They are also used to limit the number of times you see an advert as well as to measure the effectiveness of an advertising campaign. These cookies are usually placed by third party advertising networks. They remember the other websites you visit and this information is shared with third party organisations, for example advertisers.



Type of Cookie	Purpose of Cookie
Fraud detection and prevention	These cookies collect information which is used to detect and protect against fraud, theft, and abuse. The information collected relates to browser and device based information (e.g., device identifiers and metadata). It also includes information about your usage of our website and/or app (e.g., IP address, session ID, and location). As described in our Privacy Notice this information is shared with Sift, our fraud prevention partner.
Social media	These cookies allow users to share our website content on social media such as Facebook and X. These cookies are not within our control. Please refer to the respective privacy policies of the social media providers for how their cookies work.

We may also automatically collect and store certain information about your interaction with our website or app including IP address, browser type, internet service provider, referring/exit pages, operating system, date/time stamps, and related data.

Refusing or deleting cookies

Most internet browsers are set up by default to accept cookies. However, if you want to refuse or delete them (or similar technologies) please refer to the help and support area on your browser for instructions (for example: Internet Explorer, Google Chrome, Mozilla Firefox, and Safari). Please note you may not be able to take advantage of all the features of our Website, including certain personalized features, if you delete or refuse cookies.

Please visit the Network Advertising Initiative and Digital Advertising Alliance websites for additional information.

If you are a resident in the EU:

For more information on managing cookies, please visit www.youronlinechoices.eu which has further information about behavioral advertising and online privacy.

Changes to our Cookie Notice

This Cookie Notice may be updated from time to time.



APPENDIX A

We may collect the following personal information about you if you choose to provide this information to us or if we need to collect this information for the specific role you have applied for:

Category of personal information	Personal information collected
Information provided in your resumé, application form, covering letter, and during the interview process.	Your name, home address, national ID, personal email address, phone number, education, qualification, and work experience details and references or social security number (where applicable).
Information collected or created by us during the recruitment process.	Marital status, date of birth, and gender. Whether you or your spouse are a veteran or currently serving in the military. Interview notes, test scores, and correspondence between us.
Special categories of personal data.	Immigration/naturalization records which may reveal details such as citizenship status, residency permits, or visa information and right to work information such as work permits, employment authorization documents, racial and ethnic origin information, and information relating to disabilities, religious beliefs or sexual orientation, and physical or mental health information. Physical or mental health information (specifically from drug and alcohol screening) and criminal convictions.
Driver's license checks conducted if either the role applied for involves driving or as part of a remuneration or benefits package you would receive a company car or other car allowance.	Driver's license number, driver's license details (such as expiration date) and details of recent accidents, driving penalties, violations associated with that driver's license, as well as the status of the driver's license.

APPENDIX B

Country	Supervisory authority or regulatory body	
Australia	Office of the Australian Information Commissioner Level 3, 175 Pitt Street Sydney NSW 2000 Tel 1300 363 992 Email: enquiries@oaic.gov.au	Czech Republic Office for Personal Data Protection Pplk. Sochora 27 170 00 Prague 7 Tel. +420 234 665 111 Email: posta@uoou.cz
Austria	Österreichische Datenschutzbehörde Wickenburggasse 8 1080 Wien Tel. +43 1 52152 2550 Email: dsb@dsb.gv.at	Denmark Datatilsynet Borgergade 28, 5 Tel. +45 33 1932 00 Email: dt@datatilsynet.dk
Belgium	Autorité de la protection des données (APD-GBA) Rue de la Presse 35 1000 Bruxelles Tel. +32 2 274 48 00 Email: contact@apd-gba.be	Estonia Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Väike-Ameerika 19 10129 Tallinn Tel. +372 6274 135 Email: info@aki.ee
Bulgaria	Commission for Personal Data Protection 2, Prof. Tsvetan Lazarov blvd. Sofia 1592 Tel. + 359 2 915 3580 Email: kzld@cpdp.bg	Finland Office of the Data Protection Ombudsman P.O. Box 800 FIN-00521 Helsinki Tel. +358 29 56 66700 Email: tietosuoja@om.fi
Croatia	Croatian Personal Data Protection Agency Martićeva 14 10000 Zagreb Tel. +385 1 4609 000 Email: azop@azop.hr	France Commission Nationale de l'Informatique et des Libertés – CNIL 3 Place de Fontenoy TSA 80715 – 75334 Paris, Cedex 07 Tel. +33 1 53 73 22 22
Cyprus	Commissioner for Personal Data Protection 1 Iasonos Street, 1082 Nicosia P.O. Box 23378, CY-1682 Nicosia Tel. +357 22 818 456	Germany Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 53117 Bonn Tel. +49 228 997799 0; +49 228 81995 0 Email: poststelle@bfdi.bund.de



Country	Supervisory authority or regulatory body	
Greece	Hellenic Data Protection Authority Kifisias Av. 1-3, PC 11523 Ampelokipi Athens Tel. +30 210 6475 600 Email: contact@dpa.gr	Liechtenstein Data Protection Office, Principality of Liechtenstein Städtle 38 9490 Vaduz Principality of Liechtenstein Tel. +423 236 6090 Email: info.dss@llv.li
Hungary	Hungarian National Authority for Data Protection and Freedom of Information Szilágyi Erzsébet fasor 22/C H-1125 Budapest Tel. +36 1 3911 400 Email: peterfalvi.attila@naih.hu	Lithuania State Data Protection Inspectorate A. Juozapaviciaus str. 6 LT-09310 Vilnius Tel. + 370 5 279 14 45 Email: ada@ada.lt
Iceland	Persónuvernd Rauðarárstígur 10 105 Reykjavík Tel: +354 510 9600 Email: postur@dpa.is	Luxembourg Commission Nationale pour la Protection des Données 1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Tel. +352 2610 60 1 Email: info@cnpd.lu
Ireland	Data Protection Commission 21 Fitzwilliam Square Dublin 2 D02 RD28 Ireland Tel. +353 76 110 4800 Email: info@dataprotection.ie	Malta Office of the Information and Data Protection Commissioner Second Floor, Airways House High Street, Sliema SLM 1549 Tel. +356 2328 7100 Email: idpc.info@idpc.org.mt
Italy	Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 00186 Roma Tel. +39 06 69677 1 Email: garante@garanteprivacy.it	Netherlands Autoriteit Persoonsgegevens Bezuidenhoutseweg 30 P.O. Box 93374 2509 AJ Den Haag/The Hague Tel. +31 70 888 8500
Latvia	Data State Inspectorate Blaumana str. 11/13-15 1011 Riga Tel. +371 6722 3131 Email: info@dvi.gov.lv	New Zealand Privacy Commissioner PO Box 10 094, The Terrace, Wellington 6143 Tel 0800 803 909 Email: investigations@privacy.org.nz



Country		Supervisory authority or regulatory body	
Norway	Datatilsynet Tollbugata 3 0152 Oslo Tel +47 22 39 69 00 Email: postkasse@datatilsynet.no	Slovenia	Information Commissioner of the Republic of Slovenia Dunajska 22 1000 Ljubljana Tel. +386 1 230 9730 Email: gp.ip@ip-rs.si
Poland	Urząd Ochrony Danych Osobowych (Personal Data Protection Office) ul. Stawki 2 00-193 Warsaw Tel. +48 22 531 03 00 Email: kancelaria@uodo.gov.pl ; zwme@uodo.gov.pl	Spain	Agencia Española de Protección de Datos (AEPD) C/Jorge Juan, 6 28001 Madrid Tel. +34 91399 6200 Email: internacional@agpd.es
Portugal	Comissão Nacional de Protecção de Dados – CNPD Av. D. Carlos I, 134, 1º 1200-651 Lisboa Tel. +351 21 392 84 00 Email: geral@cnpd.pt	Sweden	Datainspektionen Drottninggatan 29 5th Floor Box 8114 104 20 Stockholm Tel. +46 8 657 6100 Email: datainspektionen@datainspektionen.se
Romania	The National Supervisory Authority for Personal Data Processing B-dul Magheru 28-30 Sector 1, BUCUREȘTI Tel. +40 31 805 9211 Email: anspdcp@dataprotection.ro	Switzerland	Office of the Federal Data Protection and Information Commissioner FDPIC Feldeggweg 1 CH – 3003 Berne Tel +41 (0)58 462 43 95 Email: info@edoeb.admin.ch
Singapore	Personal Data Protection Commission 10 Pasir Panjang Road, #03-01 Mapletree Business City Singapore 117438 Tel: +65 6377 3131	United Kingdom	The Information Commissioner's Office Water Lane, Wycliffe House Wilmslow – Cheshire SK9 5AF Tel. +44 1625 545 700 Email: casework@ico.org.uk
Slovakia	Office for Personal Data Protection of the Slovak Republic Hraničná 12 820 07 Bratislava 27 Tel.: + 421 2 32 31 32 14 Email: statny.dozor@pdp.gov.sk		