

The United States Privacy Statement

Established in the European Union, Admin By Request is generally not directly subject to U.S. privacy laws. However, our privacy practices, contractual commitments and technical and organizational safeguards align with comparable principles and requirements found in various U.S. state privacy laws. Where applicable, this statement outlines how we support our U.S. customers in meeting their legal obligations under their respective privacy laws and how we respect the privacy rights of U.S. residents.

We do not sell or share personal information. We only disclose personal data to our authorized sub-processors who process it on our behalf, solely for the purpose of providing and supporting our services in accordance with our Terms and Conditions and Data Processing Agreement. While we acknowledge U.S. privacy laws such as the California Consumer Privacy Act (CCPA) and similar state laws, we do not engage in activities that constitute “selling” or “sharing” personal information as defined under those laws. Because we do not use personal information for cross-context behavioural or targeted advertising, browser-based opt-out signals (such as the Global Privacy Control) will not apply.

Our U.S. Privacy Compliance

While the CCPA/CPRA has influenced the development of many subsequent U.S. state privacy laws, California is not the only jurisdiction to have enacted such regulations. Our privacy and security program is founded on the EU General Data Protection Regulation (GDPR) and internationally recognized security and privacy standards that reflect similar fundamental principles, including accountability, transparency, security, privacy and respect for individual rights.

By adhering to this framework, we maintain a level of protection consistent with the key requirements shared across U.S. state privacy laws and are positioned to help our customers meet their own compliance obligations. We provide:

- Audit and verification rights (via the DPA) - enabling customers to confirm our compliance with applicable contractual and regulatory obligations.
- Contractual commitments & role clarity (via the DPA) - defining our role as a processor/service provider, consistent with CCPA/CPRA and similar state laws, and setting out instructions, confidentiality, security measures, sub-processor flow-downs and assistance duties.
- Transparency around sub-processors and safeguards - maintaining a public list of authorized sub-processors (via our DPA) and requiring contractual safeguards.
- Public-facing privacy disclosures (via the Privacy Policy) - describing the categories of personal data processed, the business purposes for which it is used, the parties it may be disclosed to and the mechanisms available for consumer rights requests.
- Remedies & cooperation obligations (via the DPA) - committing to work with our customers to address, remediate and mitigate any identified non-compliance.

- Incident response & breach notification - providing notices, incident details and cooperation on required notifications. Timed to support state deadlines where required.
- Support for individual rights requests - assisting customers, where applicable, in responding to access, correction, deletion, portability and other rights requests made by their end-users under CCPA/CPRA and comparable state laws.
- Data minimization - processing only what is necessary to deliver the service, consistent with documented purposes and customer instructions.
- Security, retention & deletion - implementing appropriate technical and organizational measures and manage the retention and deletion of personal data in accordance with the GDPR, our agreements and the customer's instructions.
- Non-discrimination - ensuring individuals are not disadvantaged for exercising applicable privacy rights.

Privacy Across U.S. States

Privacy regulation in the U.S. continues to evolve with an increasing number of states adopting comprehensive laws governing the collection, use and disclosure of personal information. We monitor these developments closely and evaluate their requirements to ensure our practices remain aligned with recognized privacy principles in the U.S.

While our compliance framework incorporates the core elements common to U.S. state privacy laws, including transparency, accountability and audit rights, we also recognize the specific obligations our customers may have toward state residents and their individual privacy rights. We are positioned to support our customers in meeting their compliance responsibilities across U.S. jurisdictions.

The California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), have been particularly influential in shaping the modern U.S. privacy landscape, and are addressed first, followed by an overview of comparable resident rights under other state privacy frameworks to the extent they relate to our services and our customers' compliance responsibilities.

California Consumer Privacy Act (CCPA/CPRA)

California was the first U.S. state to enact a comprehensive consumer privacy law, and the CCPA, as amended by the CPRA, remains the most established framework of its kind. As it has influenced the structure and substance of many subsequent state privacy laws, it provides a useful reference point for understanding how our practices support customers in meeting their obligations under comparable regimes.

Although we are not directly bound by CCPA/CPRA, some of our customers may qualify as "businesses" under those laws. In such cases, we act as a Service Provider, which means:

- We process personal information only on behalf of customers and for purposes defined in our agreements.

- We do not use, retain or disclose personal information for our independent purposes.
- We follow our customers' instructions, the terms of our DPA and applicable laws in all processing.

Under the CCPA/CPRA, California residents have the right to:

- Access information - request details about the personal information collected, its source, purposes, disclosures and the specific data records held.
- Deletion - ask that personal information is deleted, subject to legal or operational exceptions.
- Correction - request updates to inaccurate personal data.
- Portability - obtain a copy of personal information in a portable, readily usable format (where applicable).
- Opt out - stop the sale or sharing of personal information.
- Sensitive data restrictions - limit use or disclosure of sensitive personal information, as permitted by law.
- Fair treatment - exercise rights without being discriminated against or disadvantaged.
- Appeals - challenge a refusal to act on a rights request (where applicable).

Colorado Privacy Act (CPA)

Residents of Colorado have the following rights regarding their personal data:

- Right of access - to confirm whether a controller is processing their personal data and to access that personal data.
- Right to correction - to correct inaccuracies in their personal data, considering the nature of the data and the purposes of processing.
- Right to deletion - to request the deletion of personal data concerning them.
- Right to data portability - to obtain their personal data in a portable and, where technically feasible, readily usable format that allows transfer to another entity without hindrance.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - profiling in furtherance of decisions that produce legal or similarly significant effects.

Connecticut Data Privacy Act (CTDPA)

Residents of Connecticut have the following rights regarding their personal data:

- Right to know/confirm - to confirm whether a controller is processing their personal data.
- Right of access - to access their personal data being processed.
- Right to correction - to correct inaccuracies in their personal data.
- Right to deletion - to request the deletion of their personal data.

- Right to data portability - to obtain their personal data in a portable and, where technically feasible, readily usable format.
- Right to opt out of certain processing - to opt out of processing for profiling or targeted advertising.
- Right to opt out of sales - to opt out of the sale of personal data.
- Right to opt in for sensitive data processing - to provide consent before their sensitive personal data may be processed.

Utah Consumer Privacy Act (UCPA)

Residents of Utah have the following rights regarding their personal data:

- Right of access - to confirm whether a controller is processing their personal data and to access that personal data.
- Right to deletion - to request the deletion of personal data they have provided directly to the controller.
- Right to data portability - to obtain a copy of their personal data in a format that is:
 - portable to a technically reasonable extent,
 - readily usable to a practical extent, and
 - enables the consumer to transmit the data to another controller reasonably easily, where the processing is carried out by automated means.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising, or
 - the sale of personal data.

Delaware Personal Data Privacy Act (DPDPA)

Residents of Delaware have the following rights regarding their personal data:

- Right of access - to access their personal data.
- Right to correction - to correct inaccuracies in their personal data.
- Right to deletion - to request the deletion of their personal data.
- Right to data portability - to obtain their personal data in a portable format.
- Right to disclosure of third-party recipients - to obtain a list of third parties with whom their personal data has been shared.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - profiling in furtherance of automated decisions.

Texas Data Privacy and Security Act (TDPSA)

Residents of Texas have the following rights regarding their personal data:

- Right to know/access - to confirm whether a controller is processing their personal data and to obtain that data in a readable format.
- Right to correction - to correct inaccuracies in their personal data, considering the nature of the data and the purposes of processing.
- Right to deletion - to request the deletion of personal data provided by or obtained about them.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - profiling in furtherance of decisions that produce legal or similarly significant effects, including decisions related to:
 - financial and lending services,
 - housing, insurance, or health care services,
 - education enrolment,
 - employment opportunities,
 - criminal justice, or
 - access to basic necessities, such as food and water.
- Right to non-discrimination - to not be retaliated or discriminated against for exercising their rights.

Nebraska Data Privacy Act (NDPA)

Residents of Nebraska have the following rights regarding their personal data:

- Right of access - to access their personal data.
- Right to correction - to correct inaccuracies in their personal data.
- Right to deletion - to request the deletion of their personal data.
- Right to data portability - to obtain a copy of their personal data in a portable format.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - profiling in furtherance of decisions that produce legal or similarly significant effects.

New Hampshire Data Privacy Act (NHDP)

Residents of New Hampshire have the following rights regarding their personal data:

- Right to know/confirm - to confirm whether a business is processing their personal data.
- Right of access - to access their personal data being processed.
- Right to correction - to correct inaccuracies in their personal data.
- Right to deletion - to request the deletion of personal data provided by or obtained about them.
- Right to data portability - to obtain a copy of their personal data in a portable format.

- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - certain types of automated profiling.
- Right to non-discrimination - to not be denied services, charged different rates, or otherwise discriminated against for exercising their rights.

Additional protections include:

- The right to exercise these rights free of charge at least once every 12 months.
- Businesses must respond to requests within 45 days, with a possible 45-day extension (with notice and explanation).
- Consent is required before:
 - using data outside the disclosed purposes of collection,
 - processing sensitive personal data, or
 - selling/using data for targeted advertising of consumers aged 13-15.

New Jersey Data Privacy Act (NJDPa)

Residents of New Jersey have the following rights regarding their personal data:

- Right to know/confirm - to confirm whether a controller is processing their personal data and to access that data.
- Right to correction - to correct inaccuracies in their personal data.
- Right to deletion - to request the deletion of their personal data.
- Right to data portability - to obtain a copy of their personal data in a portable, readily usable, and transferable format.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising, or
 - profiling.

Maryland Online Data Privacy Act (MODPA)

Residents of Maryland have the following rights regarding their personal data:

- Right of access - to request a copy of their personal data held by businesses.
- Right to correction - to correct inaccuracies or incomplete personal data.
- Right to deletion - to request the deletion of their personal data, subject to certain exceptions.
- Right to opt out - to opt out of the processing of personal data for:
 - targeted advertising,
 - the sale of personal data, or
 - profiling.

Nevada Online Privacy (NRS 603A)

Residents of Nevada have the following rights regarding their personal data:

- Right to opt out - to opt out of the sale of their personal data to data brokers.

Note: Nevada law does not extend additional rights similar to those found under the CCPA/CPRA or other state privacy laws.

U.S. Privacy Inquiries

Questions regarding our U.S. privacy compliance or how we support our customers in addressing applicable state privacy rights may be directed to our Data Protection Officer.

E-mail: dpo@adminbyrequest.com

Address: Admin By Request, Ved Stranden 10, 9000 Aalborg, Denmark