



Employee Privacy Notice

Title: Employee Privacy Notice

Effective Date: September 2026

Review Date: September 2027

Process Owner: Compliance

Approved by: Head of Global Risk, Compliance & Safety



Contents

1	About This Document	3
1.1	Document history	3
1.2	Contributors	3
1.3	Reviewers.....	3
2	Data Controller	3
3	Introduction	4
3.1	Purpose and scope	4
3.2	Definitions.....	4
3.3	Roles and responsibilities	4
3.4	Reviews.....	4
4	What Information Do We Collect & When Do We Collect It?	5
5	Why Do We Collect This Data?	7
6	How Do We Collect This Data?	9
7	The Legal Basis for the Collection & Processing of the Personal Data	10
8	With Whom Do We Share Your Personal Data?.....	13
9	International Transfers of Personal Data	14
10	Retention Period.....	15
11	Data Security Measures	15
12	Monitoring & IT Use	16
13	Your Data Subject Rights	16
14	Amendments to Employee Privacy Notice	17
15	Contact	17



1 About This Document

1.1 Document history

Date	Version	Release Notes	Author
August 2023	1.0		
20 October 2025	2.0		Bree Bakaric
September 2026	3.0		Bree Bakaric

1.2 Contributors

Name	Role
Bree Bakaric	Senior Data Privacy & Compliance Associate

1.3 Reviewers

Name	Role
Bree Bakaric	Senior Data Privacy & Compliance Associate
Selby Marshall	Head of Global Risk, Compliance & Safety

2 Data Controller

JOE & THE JUICE A/S (we, our, us or the Company) are committed to protecting your privacy. We, or our subsidiaries, are the data controller of the information that you provide to us.

The entity responsible for the processing of your personal data:

JOE & THE JUICE A/S

Østergade 26A, 1100 Copenhagen K

Denmark

CVR no: 26589355

www.joejuice.com

If you have any questions or requests concerning this Privacy Notice or how we handle your data, please contact our data protection team at privacy@joejuice.com



3 Introduction

3.1 Purpose and scope

This Employee Privacy Notice applies to all current & former employees, workers, freelancers, interns, contractors & other individuals recruited or hired by JOE & THE JUICE A/S or its entities & subsidiaries (excluding franchises), regardless of their employment status or location, whose personal information is collected or processed by the Company in connection with their work.

This Privacy Notice describes what personal data we collect, when and why we collect it and how we will use it. It also outlines your rights and how you may exercise your rights as a data subject.

This Privacy Notice does not cover your use of JOE & THE JUICE products or services (including the JOE App or Website) or any collection of information outside of your employment. We have a separate Privacy Notice covering the data collected from you during the Recruitment period and your use of the JOE App.

3.2 Definitions

'Personal data' means any information that can be used to, directly or indirectly, identify someone.

3.3 Roles and responsibilities

Implementing and adhering to organisational privacy policies is a collaborative effort, requiring a genuine commitment from all employees.

By being aware of one's roles and responsibilities as it pertains to JOE & THE JUICE, all relevant parties help to promote the fundamental principles of data privacy.

Responsible	Responsibilities
Joe & The Juice Compliance Team	- Yearly review & Notice Approval - Management of associated personal data privacy obligations
Joe & The Juice P&D Team	Responsible for onboarding employees with Employee Privacy Notice
Joe & The Juice Employees	Compliance with Notice

3.4 Reviews

This document shall enter into force, unless otherwise indicated on the day of its approval and shall remain valid until it is modified or revoked in a subsequent document.



This document may be repealed in whole or in part by the competent area that approved it and in a subsequent document that expressly states so in a repealing provision.

This document will be reviewed at least annually.

4 What Information Do We Collect & When Do We Collect It?

We collect a number of categories of personal data in relation to your employment with us. We collect this information throughout your employment from the moment you apply for a job during the recruitment process through to the onboarding process & up until termination.

4.1 The categories of information we collect can be categorised as follows:

4.1.1 HR information/personal identification documents

- Name, title, address, telephone number & email address
- Date of birth & gender
- Marital status & dependents
- Annual leave, personal leave, parental leave & holiday leave details
- Training history & records
- Working hours & time registration
- Retirement & benefits
- Position held within company
- Personality & cognitive ability tests, development plans
- Start & separation date
- Work performance, review details, disciplinary actions, investigations, warnings &/or grievance procedures
- Racial & ethnic origin & sexual orientation (if you choose to provide this during the application or onboarding process)
- Government-issued identification documents & numbers such as passports, licences, resident cards, national identification number, nationality/visa status, CPR or other right to work/employment eligibility documents
- Juicer ID
- Special categories of data including background checks, such as criminal offences (if applicable/required for the role you are applying for)
- Sensitive personal information (if you voluntarily disclose this to us), such as race or ethnic origin, sexual orientation



4.1.2 Professional, education or employment-related information

- Professional memberships & licences, certifications/qualifications
- Additional education or training undertaken during course of employment
- Job role & department details
- Performance records
- Any information you may have included in your CV/application, such as veteran status, photographs, career history
- KPIs (Key Performance Indicators), goals & OKR (Objective & Key Results) records
- Employee satisfaction survey results

4.1.3 Health information

- Pension information & details
- Sick leave details including doctor's notes
- Medical information, such as medical conditions or illnesses & doctor certificates when you directly report this to the Company
- Any work, health & safety incident reports
- Records relating to administering & maintaining your healthcare & other benefits
- Information about conditions needed for pensions & permanent health insurance purposes (if you leave the Company for health-related reasons)
- Sensitive health data if disclosed by a job applicant for the purposes of providing reasonable accommodation during the hiring process, such as disability status

4.1.4 Financial/economic information

- Salary details including bonuses & other compensation
- Bank account details
- Payroll records
- Social security number or other tax identifier
- Tax status

4.1.5 Geolocation data

- We may collect geolocation data about you if, for example, you are operating a Company-issued vehicle or device or access Company resources via your personal devices

4.1.6 Photographs and/or video images

- CCTV footage from offices or bars
- Photographs taken in the course of employment for identity verification & organisational charts



- Photographs or videos taken at work social events

4.1.7 Internet or other electronic network activity information

- Use of Company-issued electronic devices & networks, such as computers, tablets, phones including call-logs
- Use of Company systems & applications, hardware, resources & online information used, generated or accessed by you
- Login credentials & access logs
- Internet & other electronic activity information which is collected by cookies on our Company website & based on your cookie preferences
- Information collected via JuicerApp

5 Why Do We Collect This Data?

We ensure that any personal data collected from you throughout your employment is limited to only that which is necessary to fulfil its identified purpose.

We process & use your personal data for the following purposes:

Purpose	Examples
Recruitment & hiring	Reviewing CV, managing interview process, background/reference checks
Right-to-work verification & onboarding	Identity, immigration/visa/work permit checks
Employment contract administration	Offers, contracts, role changes, promotions
Workforce planning & scheduling	Roster management, shift swaps, availability
Timekeeping & attendance	Clock-in/out times, POS & office access, scheduling systems
Payroll & compensation	Bank details, tax IDs, salary, bonuses, equity
Benefits enrolment & administration	Health, pension, insurance, perks/benefits
Leave & absence management	Vacation, sick leave, parental leave, unpaid leave & any other leave
Health & safety management & obligations	Incident reporting, fitness for work, ergonomic assessments, workplace accommodations



Learning, training & professional development	Employee satisfaction survey records, professional certifications
Performance evaluation & management	Goals, reviews, coaching, improvement plans
Employee relations & workplace investigations	Complaints, grievances, disciplinary processes, investigation reports
Whistleblowing & ethics reporting	Case handling
Diversity, equity & inclusion initiatives	Optional self-identification where required
IT provisioning & support	Account creation, helpdesk tickets, device management, management of user account/profile
Information security & fraud prevention	Access logs, email/endpoint security monitoring
Physical security & access control	Visitor records, CCTV, electronic key management
Communications & collaboration, including offering internal communication platforms	Company email, chat, Juicer App, internal social tools
Travel & expense management	Booking details, receipts, corporate card data
Vendor & client engagement	Sharing work contact details with partners/customers
Corporate operations & reporting	Headcount analytics, budgeting, audit trails)
Compliance with laws & audits	Tax, employment, anti-money laundering, sanctions screening if relevant
Litigation & dispute management	Claim handling, legal advice, evidence preservation
Emergency preparedness	Emergency contacts, next-of-kin, critical alerts
Corporate communications & employer branding	Use of name/photo in intranet, organisation charts, newsletters
Work events, social events & wellbeing programs	Event RSVPs/attendance via JuicerApp, social initiatives
Asset management & facilities	Uniform, IT asset distribution & management
Offboarding & alumni management	Exit interviews, return of assets, references
Geolocation/vehicle telematics for work purposes	Odometer measurements & GPS



6 How Do We Collect This Data?

Most of the personal information we collect about you is provided directly by you. When we collect information from sources other than you, these sources may include:

External third parties:

- Recruitment agencies & platforms, job boards & other online assessment providers including but not limited to Hird Consulting A/S, Indeed, Recruitio, Jobindex, Glassdoor, People Test Systems, Assessio, Greenhouse Software Inc
- Referees & former employers, credit reference agencies, or other sources that supply employment verification services including background-screening vendors (to conduct references with your consent)
- Benefits providers & insurers
- Medical providers & clinicians (for fitness-to-work notes, accommodations & occupational, safety & health purposes)
- Data automatically collected through our internal IT systems (email monitoring, time tracking, etc.)
- Travel management & expense platforms
- Training & certification bodies, professional bodies & licensing authorities
- Whistleblower platform
- Internet service providers & social networks
- Government or regulatory agencies (such as tax authorities) & third-party background check providers
- Automatically collected data from Company-issued electronic devices & personal devices where you access Company resources, including but not limited to access details, audit & usage logs
- Other publicly available sources such as company registries, professional profiles, news platforms

Internal third parties:

- Colleagues
- Customer or third-party feedback
- Security & facilities systems
- IT & security tools
- Internal operational systems
- Company communications platforms
- Internal investigations & audits



7 The Legal Basis for the Collection & Processing of the Personal Data

Just as it's crucial that you understand what personal data we collect & when, it's equally as important for you to understand why we are processing that personal data. We will only process your data if we have a justifiable reason to do so in accordance with applicable personal data protection laws.

JOE & THE JUICE processes your personal data on the following bases:

1. Consent: if you have provided consent, we will process your personal data in accordance with the purpose for which you have provided consent (Article 6(1)(a) GDPR), inclusive of the following examples:

- Where you have consented to participation in campaigns, such as for social media or promotional purposes
- Where you have consented to creating content for external Company social media channels & internal Company networks
- Organisation & administration of work events, social events & wellbeing programs (where optional)
- Where you have shared photographs as a part of our Share your Moment initiative

You may withdraw your consent at any time for any personal information we collect with your consent. This includes withdrawing consent to our use of any photographs or videos taken of you at Company events for the purposes of internal corporate communications. If you withdraw the consent, this will not affect the lawfulness of the processing prior to the withdrawal. Please contact us at privacy@joejuice.com if you wish to exercise this right.

2. Contract (or pre-contract): where processing is necessary to enter into, or perform a contract with you (Article 6(1)(b) GDPR), inclusive of the following examples:

- Employment contract administration (in respect of data required to agree to & perform the contract)
- Payroll & compensation including benefits & pension administration
- Leave & absence management
- Workforce planning & scheduling (including timekeeping & attendance)
- Learning, training & professional development
- Offboarding & alumni management
- Geolocation/vehicle details for work purposes



3. Legal Obligation: where processing is necessary to comply with relevant laws & regulations (Article 6(1)(c) GDPR), inclusive of the following examples:
 - Right to work verification checks & onboarding
 - Payroll & compensation, including benefits & pension administration
 - Tax reporting
 - Compliance with legislation & regulatory audits
 - Litigation & dispute management (in respect of court/tribunal orders)
 - Health & safety management & obligations
 - Leave & absence management
 - All obligations outlined by relevant tax laws, workers' compensation laws, employment/labour laws (including laws concerning illness benefits & leave rights)
 - Workforce planning & scheduling (including timekeeping & attendance)
 - Employee relations & workplace investigations (where required by law)
 - Whistleblowing & ethics reporting (where required by law)
 - IT security & fraud prevention (where mandated)
 - Compliance with legal, regulatory or other corporate governance requirements
 - Corporate operations & reporting (for audit/statutory reports)
4. Vital Interests: where processing is necessary to protect an employee's life or physical integrity (Article 6(1)(d) GDPR), inclusive of the following examples:
 - Sharing medical information with first responders during a workplace incident
 - Emergency preparedness such as contacting an emergency next of kin in a critical situation
5. Legitimate Interests: where we process your information based on our legitimate business interests (this is always balanced against employees' rights and freedoms) (Article 6(1)(f) GDPR), inclusive of the following examples:
 - IT provisioning & support, including monitoring of systems
 - CCTV for preventing crime & ensuring safety
 - Creating IT accounts
 - Internal use of photo for internal directories, organisational charts & internal corporate communications
 - Health & safety management & obligations
 - Assessing eligibility for secondment & promotion
 - Geolocation/vehicle details for work purposes
 - Workforce planning & scheduling (including timekeeping & attendance)
 - Offering internal communication & collaboration platforms



- Learning, training & professional development including performance evaluation & management
 - General systems administration, development of IT systems & monitoring of IT accounts
 - Investigations & reporting of irregularities
 - Performance evaluation & management
 - Employee relations & workplace investigations
 - Whistleblowing & ethics reporting
 - Travel & expense management (including corporate credit card processing)
 - Vendor & client management & contact sharing
 - Corporate operations & reporting obligations
 - Litigation & dispute management including to establish, exercise or defend a legal claim
 - Emergency preparedness & collection of next-of-kin details
 - Organisation & administration of work events, social events & wellbeing programs
 - Managing OKRs, KPIs & employee satisfaction surveys
 - Asset management & facilities including physical security, access control, IT security & fraud prevention
 - Offboarding & alumni management
 - Geolocation/vehicle details for work purposes
6. Special category data: which relates to personal data we may process that is of a more sensitive nature & requires stricter processing requirements (Article 9 GDPR), inclusive of the following examples:
- Employment & social security processing to carry out obligations under relevant employment laws (Article 9(2)(b) GDPR)
 - Occupational, safety & health fitness to work assessments (Article 9(2)(h) GDPR)
 - Benefits & pension administration (Article 9(2)(b) GDPR)
 - Explicit consent given to processing of your personal information for a specific requirement (provided in an explicit, specific, informed & transparent manner) (Article 9(2)(a) GDPR)
 - Collection of sensitive personal information for equality & non-discrimination duties under relevant laws Article 9(2)(g).
7. Criminal convictions/offence data: which we only process where necessary for specific roles such as working in our airport stores or international secondments with our franchisees (Article 10 GDPR).



8 With Whom Do We Share your Personal Data?

We also disclose your personal data to our service providers, also known as data processors, which are companies & systems we use to support our business & who are bound by law & contractual obligations to keep your personal information confidential. These third parties are only permitted to use the personal data we collect for the purposes we have identified & not for their own purposes & are not permitted to share your personal data without our express permission. Where required, we enter into Data Processing Agreements or other transfer mechanisms with these third parties to ensure they only process personal data according to our direct instructions & to secure your personal data by making sure appropriate safeguards are in place.

The categories of service providers that we share personal data with & the services they provide include but are not limited to:

- **PAYROLL SERVICES PROVIDERS** that assist us in calculating and disbursing your salary and other compensation (such as ADP & Zenegy).
- **AUDITING AND ACCOUNTING FIRMS**, such as firms that assist us in the creation of our financial records.
- **PROFESSIONAL SERVICES CONSULTANTS**, such as firms that perform audits & run analytics, assist with improving our business, provide legal services, or supply project-based resources and assistance.
- **GOVERNMENT BODIES, LAW ENFORCEMENT & OTHER AUTHORITIES** that we are required to provide information to & report to under relevant legislation (tax authorities, regulatory enforcement agencies).
- **RECRUITMENT VENDORS & CONSULTANTS** that assist with the application process, including assessing candidate qualifications and providing the platform through which candidates submit their candidacy (such as Greenhouse Software Inc).
- **BENEFIT PROVIDERS & OTHER CONSULTANTS** that assist us in providing employees with pension, health insurance & other benefits (such as Soderberg & Partners & other pension funds & health schemes).
- **SECURITY VENDORS**, such as entities that assist with security incident verification & response, service notifications & fraud prevention.
- **IT VENDORS**, such as entities that assist with website design, hosting & maintenance; data & software storage; & network operation.



- **SOFTWARE SYSTEMS & SERVICE PROVIDERS** that work on our behalf to enable us to conduct general business administration & functions & day-to-day activities (including but not limited to Microsoft Outlook, Docusign, Leapsome, PeakOn, Relesys Juicer App, Attensi, e-Campus, Workplanner2, insurance companies, phone providers, corporate credit card providers, travel agencies etc.).
- **INTERNAL DEPARTMENTS WITHIN JOE & THE JUICE** (internal departments & teams).
- **JOE & THE JUICE ENTITIES & OUR PARENT COMPANY** (including other entities in connection with a corporate transaction, such as an acquisition).
- **OUR FRANCHISEES** (if the job role relates to a role operated by one of our franchisees).

When you choose to enrol in certain employee benefit programs, we share information with the external parties that we have contracted with to provide benefits to you. This disclosure is done at your direction & involves information necessary for you to enrol in the benefit program. The external parties may collect additional information about you in connection with providing the benefit & may use & share that information in ways outlined within their own privacy notices.

9 International Transfers of Personal Data

We may share personal data collected during your employment between our business entities & parent company for legitimate business purposes, which span international borders. Personal data may also be shared internationally, as outlined above in section 8, with our data processors.

If we transfer personal data to recipients in countries outside the EU/EEA, we will, if required, put in place an appropriate transfer mechanism to ensure that your data is adequately protected, for instance, by using the European Commission's standard contractual clauses for transfers of personal data to non-EU/EEA countries or relying on our processors' self-certification to the EU-US Data Privacy Framework. Wherever your personal information is transferred, stored or processed by us, we will take appropriate technical & organisational measures to protect your personal information, in accordance with relevant privacy laws.



10 Retention Periods

Personal data collected will only be stored for as long as is reasonably necessary & proportionate to accomplish the purposes for which it was collected & processed. Whilst stored, this information will only be accessible on a restricted basis by certain employees on a need-to-know basis.

Generally, the following retention periods will be adhered to:

Type of personal data	Retention Period
Employee personal information related to administration, compensation, benefits, grievance procedures & investigations	10 years post termination of employment
Results of personality & cognitive assessments collected during recruitment phase (governed by our Recruitment Privacy Notice)	Length of employment
Airport security clearances	1 year post termination
Attendance at social events	1 year post event
CCTV footage	In accordance with our CCTV Privacy Policy (differs by country)
References	1 year post termination
Administration of Juicer App & social attendances	3 months post termination
Share your Moment photos	Photos kept indefinitely as per terms & conditions (due to potential use in stores)

11 Data Security Measures

Whilst stored, your personal data is subject to a number of technical & organisational security measures used to protect your information & prevent unauthorised access, alteration, disclosure or loss. Examples of these include access restrictions, password protection, multi-factor authentication, information security policies, SSO, network protection & endpoint security, logging & monitoring to detect misuse, secure software change & backup processes, data minimisation & other safeguarding measures employed by us internally & by our data processors (who are contractually bound via Data Processing Agreements & where relevant, international transfer safeguards). We also maintain an incident response process to investigate, mitigate & notify you of any privacy breaches, as required by law.



12 Monitoring & IT Use

IT systems, devices (such as iPads, computers & mobile phones), networks & apps provided to employees by JOE & THE JUICE for work purposes may be monitored & usage logged in order to protect our people, customers & assets, meet regulatory/legal

duties & investigate any suspected misconduct or security incidents. This includes, but is not limited to, phone calls, email, chat, calendars, file storage, internet usage/access & VPN. CCTV may also be monitored in accordance with our CCTV Policy.

All monitoring is proportionate & targeted to the purpose & only conducted in accordance with lawful means. Content is only accessed where necessary.

Where permitted (as per the Company's Acceptable Use of IT Equipment Policy & Information Security Policy), personal use of company devices & systems is allowed, but employees should have no expectation of privacy when using company resources.

13 Your Data Subject Rights

Under GDPR, data subjects hold the following rights in relation to their personal data:

1. Right to be *Informed*: you have the right to be told how your personal data is collected, why it is being processed, who it is shared with & how long it will be kept.
2. Right of *Access*: you can request a copy of your personal data held by us, along with details of how it is being processed.
3. Right to *Rectification*: if your data is inaccurate or incomplete, you can ask us to correct or update the information we hold.
4. Right to *Erase*: you can request that we delete your personal data when it is no longer needed or if you withdraw consent (please note that certain exceptions apply in accordance with legal obligations).
5. Right to *Restrict Processing*: you can limit how your personal data is used in certain situations.
6. Right to *Data Portability*: you can request that your personal data be provided to transfer to another organisation.
7. Right to *Object*: you can object to how we process your personal data for direct marketing or under legitimate interest grounds.



8. Rights related to Automated Decision-Making & Profiling: you have the right not to be subject to a decision based solely on automated processing if it has legal or significant effects on you & you can request human review in such cases (we note that we do not engage in solely automated decision-making in any employment-related decisions).

US residents can find their rights & a disclosure in accordance with the *relevant US privacy laws* at Appendix A.

All data subject access requests for personal data should be made in writing to privacy@joejuice.com. There may be conditions or limitations on these rights. This depends on the specific circumstances of the processing activity. We will assess each request & respond within the required timeframes.

You may always lodge a complaint about how your personal data is being processed with your relevant data protection supervisory authority. Appendix B contains a list of the relevant data protection supervisory authorities in relation to each country in which we operate our wholly owned JOE & THE JUICE entities.

14 Amendments to Employee Privacy Notice

We may amend this notice from time to time. If we do so, an updated version will be available on our internal intranet. You are responsible as an employee for regularly reviewing this Notice so that you are aware of any changes to it.

15 Contact

Please contact us via privacy@joejuice.com if you have any questions regarding the protection of your personal data or if you wish to exercise your legal rights.



APPENDIX A

U.S. CONSUMER PRIVACY RIGHTS

This appendix supplements the Employee Privacy Notice and applies to individuals located in U.S. states that have enacted a comprehensive consumer privacy law, including, California, Minnesota, Maryland, Texas, Virginia and New Jersey. If you are a resident of one of these states, this Appendix describes the additional rights you may have regarding your personal information and how to exercise them. Where a right or process differs by state, we have noted this below.

YOUR PRIVACY RIGHTS

Depending on where you live, you may have the following rights regarding your personal information:

- 1) *Right to Access*: you have the right to request access to personal information we hold about you.
- 2) *Right to Correct*: you have the right to ask us to correct any inaccurate personal data we hold about you.
- 3) *Right to Erasure*: you have the right to ask us to delete personal information we've collected from or about you, subject to some exceptions, such as where we are required to keep it for legal reasons.
- 4) *Right to Data Portability*: you have the right to request a copy of your personal information in a portable format that's readily usable, where technically feasible.
- 5) *Right to Opt-Out of Sale or Sharing*: we do not sell your personal information for money, however, if you have opted to receive remarketing via the JOE App, we may share your personal information with some of our advertising partners. You may have the right to opt-out of your personal information being shared for the purposes of targeted advertising by managing your consent preferences in our JOE App.

HOW TO EXERCISE YOUR RIGHTS

You can submit a request by emailing privacy@joejuice.com. We will need to verify your identity before completing most requests.

When you submit a request exercising your rights, we'll acknowledge it within 10 business days & respond substantively within 45 days. If we need more time (up to 90 days), we'll notify you in writing.



Only you or an authorised agent may submit a verifiable request related to your personal information. Agents must have written permission, & you'll need to verify your identity with us. We will verify both your identity & the agent's authority using the personal information provided. You don't need to create an account to make a verifiable request. If necessary, we may ask for at least two pieces of personal information to ensure accuracy & prevent fraud. We'll compare this information to what we hold to verify your request

RIGHT TO APPEAL

If we decline to act on your request, you may appeal by contacting us at privacy@joejuice.com. We will respond to your appeal typically within 45 days. If your appeal is denied, some states allow you to lodge a complaint with your state Attorney General or applicable data protection authority.

ADDITIONAL DISCLOSURES FOR CALIFORNIAN RESIDENTS

If you are a California resident, the California Consumer Privacy Act (as amended by the California Privacy Rights Act) gives you the rights above, plus the following:

- 1) *Right to be Informed*: you have the right to confirm whether we process your personal information.
- 2) *Notice at or before collection*: before we collect your personal information, we will advise you of the categories collected and the purpose for processing. We describe the categories of personal data we process about you and the purposes for which we process this information above in the substantive part of this Privacy Notice.
- 3) *Right to non-discrimination*: you have the right to non-discrimination, meaning that we won't deny you goods or services, charge you a different price, or provide a different level of service because you have exercised any of the above rights. We may, however, charge different prices, or provide a different good, if that difference is reasonably related to the value provided to us by your personal information. For more information in relation to this, see our [Notices of Financial Incentive for Memberships](#) and [Notice of Financial Incentive for the Loyalty Program](#).
- 4) *Right to Limit Use of Sensitive Information*: we do not collect, process or disclose sensitive information for any purpose other than what is permitted under applicable law for our business operations or recruitment purposes. As such, we are not required to offer customers a 'Right to Limit' the use or disclosure of sensitive personal information.



CONSUMER HEALTH DATA RIGHTS IN WASHINGTON

You may have additional rights relating to your consumer health data in Washington, detailed in our [Washington Consumer Health Data Privacy Notice](#).

CHANGES TO THIS APPENDIX

We may update this appendix from time to time to reflect changes in the law or our practices. The Notice date at the top of this Privacy Notice will show when this Appendix was last revised.



APPENDIX B

DATA PROTECTION SUPERVISORY AUTHORITIES

COUNTRY	SUPERVISORY AUTHORITY/ENTITY	CONTACT DETAILS
Denmark	Datatilsynet	https://www.datatilsynet.dk dt@datatilsynet.dk 33 19 32 00
Norway	Datatilsynet	www.datatilsynet.no postkasse@datatilsynet.no 22 39 69 00
Sweden	Integritetsskyddsmyndigheten (IMY)	https://www.imy.se imy@imy.se 08 657 61 00
United Kingdom	Information Commissioner's Office (ICO)	https://ico.org.uk 0303 123 1113
USA	No single federal authority	
France	Commission Nationale de l'Informatique et des Libertés (CNIL)	https://www.cnil.fr/en/home 01 53 73 22 22
Belgium	Autorité / Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/burger/acties/contact contact@apd-gba.be +32 (0)2 274 48 00
Germany	BfDI (federal) + 16 Länder-level DPAs	http://www.bfdi.bund.de/ oistsekke@bfdi.bund.de +49 (0)2228 997799 0



Switzerland	Federal Data Protection and Information Commissioner (FDPIC)	https://www.edoeb.admin.ch/en 058 462 95
Netherlands	Autoriteit Persoonsgegevens (AP)	https://www.autoriteitpersoonsgegevens.nl +31 (0)88 1805 250
Finland	Office of the Data Protection Ombudsman (Tietosuojavaltuutettu)	https://tietosuoja.fi/etusivu +358 (0)29 566 6777