JOE & THE JUICE - CCTV POLICY

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

When you visit our bars or gym, purchase our products, or otherwise communicate with us, JOE & THE JUICE will, as the data controller, collect & process personal data about you. As data controller, we are responsible for determining the means & purposes for processing data captured on CCTV.

This policy applies to your visit in a JOE & THE JUICE Bar ("**THE BAR**"), the JOE & THE JUICE Gym ("**JOE GYM**") & JOE & THE JUICE global offices. It does not refer to, or deal with, the collection & use of your personal data in relation to JOE & THE JUICE's mobile application which is governed by separate Terms & Conditions & Privacy Policy available here or JOE & THE JUICE related websites & our social media accounts which is governed by separate Terms & Conditions & Privacy Policy available here. This policy does not apply to use of CCTV by our franchise partners in their stores.

The use of CCTV systems will be conducted in a professional, ethical & legal manner & any diversion of the use of CCTV from his policy is prohibited. The Policy outlines the purposes for which we use CCTV & how we will process data recorded by CCTV in accordance with all applicable data protection laws & best practice.

DATA CONTROLLER

The entity responsible for the processing of your personal data via CCTV is:

JOE & THE JUICE A/S

Østergade 26A, 1100 Copenhagen K
DENMARK
CVR no: 26589355
www.joejuice.com
For inquiries about our processing of your personal data, contact us at: privacy@joejuice.com

1. WHAT INFORMATION DO WE COLLECT & HOW DO WE USE IT?

Generally speaking, we will collect some of your personal data whenever you interact with JOE & THE JUICE.

When you attend a JOE BAR, the JOE GYM, or one of our offices as a visitor, contractor, or employee, you may be subject to CCTV recording, which will collect the following:

- Image
- Location & time data

No audio will be recorded by our CCTV devices.

We collect this data via CCTV for the following purposes:

- Ensuring the safety of persons visiting our premises by enhancing our security, including for the prevention of crime
- Managing complaints from any individuals, including for the purposes of investigation of crime & defence of any possible insurance & legal disputes/litigation
- Checking employee misconduct for the purposes of internal disputes & investigations (including confirmation of employee working hours & leave requirements in the US)
- Monitoring the progress of construction-related projects
- Ensuring the arrival of deliveries

We ensure that footage recorded via CCTV is limited to only that which is necessary to fulfil its purpose.

2. 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 the applicable data protection law.

We consider the following legal bases to apply for our collection of your data via CCTV recording:

Purpose	**Legal Basis**	**Applicable law**
Safety of persons & premises & prevention of crime	Legitimate interest	GDPR Article 6(1)(f)

Managing internal & external disputes & investigations	Legitimate interest Necessary for the establishment, exercise or defence of legal claims	GDPR Article 6(1)(f) GDPR Article 9(2)(f)
Monitoring construction projects & contractor work	Legitimate interest	GDPR Article 6(1)(f)
Monitoring deliveries	Legitimate interest	GDPR Article 6(1)(f)

Special category data is not intentionally collected within the EU. If incidentally captured, processing will only occur under an applicable Article 9 GDPR condition, such as 9(2)(f).

3. LOCATION OF CCTV

Cameras are located in areas where we have identified a need & where other solutions are ineffective or impractical. Cameras are not used in areas where the subject has a heightened expectation of privacy, such as change rooms/bathrooms, employee break areas or the JOE GYM wellness area.

Our CCTV system is used solely for the purpose(s) identified above & is not used to routinely monitor employees, visitors or staff.

We will make every reasonable effort to be transparent about our use of CCTV & inform data subjects of the presence of CCTV cameras by installing prominent signage in premises where CCTV is in use.

In the event that we open a new location, any CCTV installed in the premises will be done in accordance with this policy.

4. DISCLOSURE OF YOUR PERSONAL DATA

We also disclose personal data to service providers, which are companies we use to support our business & who are bound by law & contractual obligations to keep your personal information confidential. We share your personal data captured on CCTV with our third-party service providers/data processors for the purposes of recording & storing the images.

When data is shared with, or transferred to, service providers on behalf of JOE & THE JUICE, we will take all measures reasonably necessary to ensure that your data is processed solely for the purposes outlined in this policy, & that such data is processed in a secure manner.

Disclosure of CCTV footage may also be authorised by us if it is required for the purpose with which the recording was taken, such as disclosure to law enforcement agencies, security management, investigators, & insurance companies.

Subject to this policy, we will not share any CCTV recordings with a third party, except where we are required to do so under law or a court order.

5. ACCESS TO CCTV FOOTAGE

CCTV footage will only be accessible by authorised personnel, which may include security staff, law enforcement, & internal employees on a need-to-know basis (e.g.to manage employee misconduct/investigations, ensure fulfilment of deliveries & monitor progress of construction projects).

Recorded images are viewed when there is suspected criminal activity & not for routine monitoring of visitors. CCTV is checked to investigate employee misconduct & to ensure employees' time recording is accurate for legitimate business purposes.

6. INTERNATIONAL TRANSFERS OF PERSONAL DATA

We may share personal data recorded on CCTV between our business entities for legitimate business purposes, which span international borders. Personal data may also be shared internationally, as outlined above in section 4, with our data processors.

If we transfer personal data to recipients in countries outside the EU/EEA, we will, if required, put a contract or other means in place 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 commercially reasonable steps to safeguard the privacy of your personal information.

7. STORAGE & RETENTION

CCTV recordings captured will not be retained indefinitely but will be deleted once there is no purpose for us to retain the information.

The recordings will be stored securely on the local hard disk of our CCTV provider & will be accessible via our provider's cloud software. CCTV footage 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:

Country	**Retention Period**
Denmark	30 days if footage is obtained for crime-preventing purposes, otherwise 72 hours
Sweden	72 hours
Norway	7 days unless recordings are to be used for an investigation, upon which recordings can be retained for 30 days. Recordings can be kept up to 3 months if they include recordings of the till. *Working Environment Act chapter 9 cf. Camera Surveillance Regulation*
Finland	30 days
France	30 days
United States	30 days
United Kingdom	30 days
Germany	72 hours
Switzerland	30 days
Netherlands	28 days
Belgium	30 days

In circumstances where an incident occurs, including personal injury incidents, which have been captured on CCTV recordings, we may consider it reasonably necessary to keep the footage for a longer period than stipulated above, in order to protect our lawful interests or assist in internal/external investigations. If we keep CCTV recordings for longer than the stipulated period in the table above, we will document the reason for retaining the footage. This may include keeping the footage for the duration of a limitation period under law for potential personal injury claims (where an incident has occurred), in order to protect our legal interests in investigating & /or defending the claim. Other reasons for retaining CCTV footage for longer than the above stipulated retention periods include, but are not limited to, court orders, third-party preservation notices & /or other litigation.

Whilst stored, your personal data is subject to a number of technical & organisational security measures employed to protect your information. Examples of these include access restrictions, password protection, multi-factor authentication, information security policies & other safeguarding measures employed by our data processors.

8. DATA SUBJECT RIGHTS

Under relevant privacy laws, data subjects may object to the processing of their personal data or make a request for access, rectification or erasure of their personal data, including CCTV recordings. You also hold the right to lodge a complaint with your country's relevant data protection agency about our handling or processing of your personal data.

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 used.
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 *Erasure*: 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 your & can request human review in such cases (we note that we do not engage in solely AI based decision-making throughout the recruitment processes).

Californian residents can find their rights & a disclosure in accordance with the *California Consumer Privacy Act* as amended by the *California Privacy Rights Act* at Appendix A.

All data subject access requests for CCTV footage should be made in writing to privacy@joejuice.com & specify the location of the recording together with the date & time & any identifying information.

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.

We reserve the right to anonymise or redact the identity of third parties visible in CCTV recordings. If third parties are identifiable in footage that you request, we will balance your rights to access with those of the third party.

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 subsidiaries.

9. AMENDMENTS TO THE POLICY

We may amend this notice from time to time. If we do so, an updated version will be available within the JOE & THE JUICE website (www.joejuice.com). You are responsible for regularly reviewing this Policy so that you are aware of any changes to it.

10. 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.

This Policy is available in alternative formats upon request for individuals with disabilities.

Effective: September 2025 (Version 1)

APPENDIX A

CALIFORNIAN RESIDENTS' DISCLOSURE

The entirety of this Privacy Notice applies to Californian residents, in addition to this appendix.

We do not sell or share your personal information with third parties for targeted advertising, as part of recruitment, employment, or personnel management processes, in compliance with the *California Consumer Privacy Act* as amended by the *California Privacy Rights Act*.

If you're a California resident requesting access to your information, please specify if you want to access categories of personal information categories or specific pieces of personal information. California residents can opt-out of any sale or sharing of personal information for targeted advertising, although we do not engage in such practices. We also do not use sensitive personal data beyond business operations or recruitment purposes.

Californian residents have the following rights in relation to the personal data we process about them: right to know & access & data portability, right to delete, right to correct inaccurate information, right to opt out of sale and sharing of personal information, right to limit use & disclosure of sensitive personal information & the right to non-discrimination.

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.

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