Biometric Data Policy — Identity Verification

Effective October 15, 2026 · v1.1.0

Dealr, Inc. (“**Dealr**,” “we,” “us”) uses a face check to confirm a person’s identity in two places. Some businesses that use Dealr to sign documents electronically, such as vehicle dealerships (this policy calls each one “**the business**”), ask signers to complete a face check before they sign. A business may also ask a customer to complete the same face check at another step of a transaction, such as a test drive agreement, a credit application, or a digital deal (a “**transaction check**”). Dealr may also ask people who use Dealr’s software, such as dealership staff, to complete the same face check to verify their identity for their account, or before they reset their account or regain access to it (an “**account check**”). This policy explains what the face check collects, what it is used for, how long the data is kept, and how it is destroyed. It is Dealr’s written biometric data policy, published for anyone to read as the law requires.

The short version

- Before you sign, you may be asked to complete a face check. It compares a live image of your face with the photo on your driver’s license or ID.
- The check is used to verify that the person signing matches their ID. For some signers, we also keep the check’s scores for up to 90 days, only to measure how accurately the check works.
- The check runs only after you check a box agreeing to it. If you don’t want a face check, you can arrange to sign another way with the business, such as in person.
- Amazon Web Services (AWS) runs the check as our service provider. The video of your face goes straight from the camera to AWS. AWS saves one still image from it in a private, encrypted storage area that Dealr controls, and compares that image with the photo on your ID. Dealr’s software never opens the image. We delete it as soon as the check is done, and it is never kept more than 1 day.
- The photos you take of your ID do go to Dealr’s servers. We use them to read your ID, to cut out the photo of your face on it for the comparison, and to file a copy of your ID with your signature record. We delete the photos themselves when the check ends, and never keep them more than 1 day.
- We keep the result of the check (for example, whether your face matched your ID), a copy of the ID you showed, and a certificate that records the check, with your signature record. The business you are signing with receives the result and can see the copy of your ID and the certificate. The business never receives the live images of your face, any face measurements, or the check’s scores.
- A business may also ask you to complete the same face check for a test drive agreement, a credit application, a digital deal, or another step of a transaction with it. It works the same way, and we keep no images of your face and no scores from it. We keep the result. If the business wants a copy of your ID for its records, we give it one, and that copy is the business’s record, not ours.
- If you use Dealr’s software, for example at a dealership, we may ask you to complete the same face check to verify your identity for your account, or before you reset your account or get back into it. It works the same way and follows the same rules, we keep no scores and no copy of your ID from it, and you can ask an administrator at your business to confirm it’s you instead. If it passes,

we keep your legal name from your ID, encrypted, to recognize you next time. The business you work for never receives your face data.

- Signing in with your device's face or fingerprint unlock (a passkey, such as Face ID or Windows Hello) is different: the match happens on your device, and Dealr never receives your face or fingerprint data.
- We never sell, lease, or trade your biometric data, and we never profit from it.

---

1. What this policy covers

This policy covers the face check in Dealr's electronic signing services, the same face check when a business uses it for a transaction check, and the same face check when Dealr uses it for an account check. It applies to anyone who completes the check, whether in person on a device at the business or remotely on their own phone or computer. The face check is not offered in person at business locations where local law does not allow it, and account checks are not offered to people who work for a business located there.

This policy does not cover signing in with a passkey that uses your device's built-in face or fingerprint unlock (such as Face ID, Touch ID, or Windows Hello). That match happens entirely on your device. Dealr receives only a confirmation that your device unlocked the passkey, never an image of your face, a fingerprint, or any measurement of them, so Dealr collects no biometric data when you use one.

In this policy, "**biometric data**" means the live images of your face captured for the check and the measurements of face geometry made from them and from the photo on your ID. It also means the check's scores described in Section 2, which are calculated from those measurements. We treat the scores as biometric data whether or not a particular law does. Biometric data includes anything that state law treats as a "biometric identifier" or "biometric information."

This policy does not cover the other information in your transaction, such as your name, address, or the documents you sign. The Consumer Privacy Notice covers that information.

The laws this policy is written for include 740 ILCS 14 (Illinois), Tex. Bus. & Com. Code §503.001 (Texas), RCW 19.375 and RCW 19.373 (Washington), C.R.S. §6-1-1314 (Colorado), and Cal. Civ. Code §1798.140 (California).

---

2. What we collect and what we don't

What the face check collects:

- **A live video of your face.** The camera on the device records a short video of your face while you follow the instructions on the screen. It is used to check that a real person is in front of the camera, and not a photo, a screen, or a mask. AWS takes one still image of your face from the video for the comparison.
- **Photos of the front and back of the driver's license or ID you present.** You take them with the camera on a phone or tablet. They are sent to Dealr's servers. Our software reads the barcode on the back. AWS reads the printed details on the front and finds the face in the photo on your ID. Our software then cuts out that part of the photo, checks that it is clear enough to compare, and sends the cut-out photo to AWS for the comparison. While the check runs, we hold the photos of your ID in a private, encrypted storage area that Dealr controls (Section 6).

- **Face measurements.** To compare the still image with the photo on your ID, AWS measures the geometry of both faces. The measurements are used only for that comparison, inside AWS. They are not saved as a face template. While you take the check, the AWS software running on your device also finds your face in the camera view to guide you. Nothing from that is saved on the device.
- **Scores.** The check produces two scores: how confident it is that a real person was in front of the camera (the liveness score), and how similar your face is to the photo on your ID (the similarity score).

What we don't collect or do:

- We do not collect fingerprints, voiceprints, iris or retina scans, or hand geometry.
- We do not keep the live video or the still image of your face, and no face template is saved. Section 6 explains when each is destroyed. We do not add your face to any database or collection of faces.
- We do not search your face against other people's faces. The check compares your face only with the photo on the ID you present.
- We do not use your face data to guess your age, gender, race, emotions, or health.
- We do not use your face data to track you or to recognize you later.

How the check is decided: the check passes only if the liveness score is at least 0.90 and the similarity score is at least 0.90, on a scale from 0 to 1. These thresholds are fixed. We change them only by updating this policy.

What we keep: the results of the check, as part of the record of your signature:

- whether your face matched the photo on your ID (yes or no);
- whether the check found a real person in front of the camera (yes, no, or unable to tell);
- how the match was decided: the two fixed thresholds the check applied, and the versions of the liveness check and of the face-comparison service it used;
- the date and time of the check, and an identifier for the check session;
- the document you signed after the check; and
- the record of your agreement to the check: who agreed, which version of the consent screen and of this policy was shown, when, and the device and internet address used;
- how the details printed on your ID compared with the details the business has on file for you, with most of each detail hidden (for example, only the last four digits of your ID number);
- your answer to any question about where you are when you take the check (Section 4);
- a tamper-evident log of the steps above, which cannot be changed after it is written; and
- an identity verification certificate: a document filed with your signature record that shows the results and the copy of your ID.

The results do not include the scores or any image from the live video. They cannot be used to recreate an image of your face from the live video or to run another face match.

Scores kept for up to 90 days, for some signers: for some signers, we keep the liveness and similarity scores for up to 90 days, only to measure how accurately the check works. With them we keep the thresholds, the outcome, image-quality readings for the ID photo (such as sharpness and brightness), codes that explain why a check could not finish, and the states described below. Apart from the scores, these items are not biometric data.

- We look at up to three states: the state in the address the business has on file for you, the state in the address on your ID, and the state that issued your ID.
- We keep the scores only if we know at least one of these states and none of them is a state with a law that specifically regulates biometric data or treats it as sensitive personal data.
- If any of these states has such a law, or we don't know any of them, we never keep the scores.
- We treat the scores as biometric data. We keep them apart from your signature record, and the business never receives them. They cannot be used to recreate an image of your face or to run another face match.
- If you ask what information we hold about you, or ask us to delete it, your request covers the scores (Section 8).

The copy of your ID: we also keep a copy of the front and back of the driver's license or ID you presented for the check, with the record of your signature. It is kept as a document, like a photocopy of your license, and the business you are signing with can see it. The certificate described above includes this copy, and the business can see the certificate too. If the business has no copy of your ID on your customer record, we also place one there; that copy is the business's own record, and the Consumer Privacy Notice covers it. We never use any copy of your ID for biometric purposes: we do not run face checks on it or make face measurements from it. Section 6 explains how long it is kept.

Transaction checks: a transaction check collects the same things as the face check for signing, in the same way, and decides the result with the same thresholds. We never keep the scores from a transaction check, and we keep no copy of your ID for ourselves. In Dealr's records, we keep the result of the check (whether it passed, the thresholds, the versions of the services used, and when it ran), the record of your agreement, and a log of the check's steps. If the business wants a copy of the ID you presented, we give it one for the business's own records; the Consumer Privacy Notice covers that copy. Neither we nor the business use it for biometric purposes.

Account checks: an account check collects the same things as the face check for signing, in the same way, and decides the result with the same thresholds. We never keep the scores from an account check, and we keep no copy of the ID you present for it. With your account's security records, we keep:

- the result of the check (whether it passed, the thresholds, the versions of the services used, and when it ran), the record of your agreement, and a log of the check's steps;
- a masked summary of your ID that shows whether each detail matched your account, with only the first letter of each part of your name, the last 3 digits of your ID number, your birth year, the month and year the ID expires, and the first 3 digits of your ZIP code;
- a one-way code made from your date of birth and name, so that a later check can be compared with this one. It cannot be turned back into your date of birth or name; and
- if the check passes and you don't have a verified identity yet, your "**verified identity**": your legal name as it appears on your ID (encrypted), the type of ID, the state that issued it, and a one-way code made from your date of birth. Later account checks are compared with it. Your verified legal name changes only through a name-change request that you confirm with a new account check.

We never keep your ID number, your full date of birth, or any image of your ID or your face from an account check. None of the items above is biometric data: none is made from the images of your face, and none can be used to recreate an image of your face or to run a face match.

3. Why we use it

We use the face check only to verify that the person signing a document matches their ID, and that a real person is present when the document is signed. For a transaction check, we use it only to verify that the person completing that step of the transaction matches their ID, and that a real person is present.

For an account check, we use the face check only to confirm that the person verifying, resetting, or regaining access to a Dealr account is the person the account belongs to, to protect the account and the information in it. An account check runs only when:

- you choose to verify your identity for your account;
- you reset your password, or regain access to your account after losing the device you use for two-step verification;
- someone asks to recover your account or change its sign-in details, such as its email address or phone number; or
- you have administrator access at your business and Dealr requires a verified identity for that access. You have 14 days to complete it, and an administrator can confirm your identity instead (Section 4).

An account check is never part of signing in normally.

For some signers, we also keep the check's scores for up to 90 days to measure how accurately the check works (Section 2). We use what we learn only to decide whether the check's fixed thresholds should change. Any change is made by updating this policy.

We do not use biometric data for any other purpose. We do not use it for marketing or advertising, to train artificial intelligence models, to monitor employees or track their work, or to control access to buildings or devices. If we ever want to use biometric data for a different purpose, we will tell you first and ask for your agreement again.

4. Your agreement comes first

The face check never starts without your agreement. Before the camera turns on, a separate screen explains what the check is for, how long your face data is kept, and when we keep the check's scores, and links to this policy. The box on that screen starts unchecked. The check runs only after you check the box and continue.

When you agree, we record who agreed, which version of the consent screen and of this policy was shown, the date and time, and the device and internet address used. Where local law limits face checks at businesses open to the public, such as in Portland, Oregon, we may also ask where you are before the check starts, and we record your answer. Checking the box is your written release for the face check, for keeping the scores as Section 2 describes, and for the disclosure of your biometric data to AWS (Section 5).

Only electronic signing through Dealr requires the face check. If you don't want to complete it, don't check the box, and contact the business to arrange to sign another way, such as in person. You can do the same if the check does not confirm that you match your ID. Declining the face check does not stop you from completing your transaction with the business.

A transaction check works the same way: the same screen comes first, and checking the box is your written release. If you don't want a face check, or it does not confirm a match, don't check the box, and ask the business to confirm your identity another way, such as by looking at your ID in person. Declining does not stop you from completing your transaction.

An account check works the same way: the same screen comes first, and checking the box is your written release. Dealr, not the business you work for, asks for the account check. If you don't want a face check, or it does not confirm a match, you can confirm your identity another way: another administrator at the business you work for can confirm who you are in Dealr, with a written note, in place of the face check. Any other approval your request needs, such as approval by Dealr, still applies. If no other administrator at your business can confirm it, Dealr's security staff handle your request. Declining does not lock you out of your account. For a business located where local law does not allow face checks, such as Portland, Oregon, no account check is offered, and confirmation by an administrator takes its place.

---

5. Who receives it

Amazon Web Services. Amazon Web Services, Inc. ("AWS") runs the face check for us as our service provider, using its Amazon Rekognition service. AWS also hosts the private storage area where the still image of your face is held until we delete it. AWS also reads the printed details on the front of your ID with its Amazon Textract service. Those details are not biometric data, and the Consumer Privacy Notice covers them. Dealr's software never opens, downloads, or displays the live images of your face. AWS may use your biometric data only to run the check and hold the storage area for us. It does not keep your biometric data for its own purposes or use it to develop or improve its services.

Microsoft. If our software can't read the barcode on the back of your ID, Microsoft's Azure AI Document Intelligence reads it for us as our service provider. The back of your ID is not biometric data, and the Consumer Privacy Notice covers it.

The business you are signing with. The business receives the result of the check (the items listed under "What we keep" in Section 2) and can see the copy of your ID and the certificate. If you decline the face check or it does not confirm a match, we tell the person at the business who sent you the documents, without any face data. The business never receives the live images of your face used for the check, any face data, or the check's scores. If you take the check in person on the business's device, its screen shows the camera view while you take the check, but the business's software never receives the images.

The business (transaction checks). The business receives the result of the check and, if it wants one, a copy of the ID you presented, which becomes the business's own record. If you decline the face check or it does not confirm a match, we tell the business, without any face data. The business never receives the live images of your face, any face data, or the check's scores.

What the business may not do with the result. A business that uses the face check for signing or a transaction check agrees with Dealr not to use the result, or your decision to decline the check, to decide whether to give you credit or a lease, on what terms, or whether to do business with you. If the check does not confirm a match, the business must confirm your identity another way.

The business you work for (account checks). The business never receives the images of your face, any face data, or a copy of your ID from an account check. Its account administrators can see whether an account check passed or failed, whether you have a verified identity, and your name as it appears on your ID with only your middle initial (for example, "Robert J. Smith"). If you report

a lost device or someone asks to recover your account, they also receive an email about it. Dealr's support staff can see the same things. Only Dealr's security staff can see your full legal name.

No one else. We do not disclose biometric data to anyone else unless a law, or a valid warrant or subpoena issued by a court, requires it.

No selling or profiting. We never sell, lease, or trade biometric data, and we never otherwise profit from it.

---

6. How long it's kept and how it's destroyed

Data	Where it is held	When it is destroyed
The live video of your face	Streamed from the camera straight to AWS. Nothing is saved on the device or on Dealr's servers	AWS makes its data for the check session unavailable 3 minutes after the session is created
The still image of your face taken from the video	A private, encrypted storage area that Dealr controls, hosted by AWS. Dealr's software never opens or downloads it	We delete it as soon as the comparison is done, pass or fail, or as soon as the check ends without one. If a deletion fails, we retry it. An hourly cleanup also removes anything left, no later than 1 day after it was saved
The face measurements made for the comparison	Inside AWS only, while the comparison runs	Not saved. No face template is kept
The photos of the front and back of your ID taken for the check	Dealr's servers while they are processed, and a private, encrypted storage area that Dealr controls, hosted by AWS	We delete them when the check ends: once it passes and the copy of your ID is filed, or when you retake the photos, the check is locked, or it starts over. An hourly cleanup also removes anything left, no later than 1 day after it was saved
The photo of your face cut from your ID for the comparison	Dealr's servers, in memory only, while it is prepared and sent to AWS	Not saved. Where the photo sits on your ID is not recorded either
The check's scores, for the signers described in Section 2	Dealr, kept apart from the record of your signature	90 days after the check, or sooner if you ask us to delete them (Section 8)
The results of the check, the record of your agreement, the log of the check's steps, and the certificate (Section 2)	Dealr, with the record of your signature	Kept with the signature record for as long as it is kept, which is at least seven years after signing (the E-Sign Consent explains why). The results, the certificate, and the record of your agreement are deleted when the signature record is deleted, for example under our agreement with the business after its account with Dealr ends. The log of the check's steps cannot be changed or deleted, so it stays; it holds no images of your face, face measurements, or scores
The copy of your ID (Section 2)	Dealr, with the record of your signature	Same as the results of the check
The results of a transaction check, the record of your agreement, and the log of its steps (Section 2)	Dealr	3 years after the check, then deleted

Data	Where it is held	When it is destroyed
A copy of your ID given to the business after a transaction check	The business, as its own record	Kept and deleted by the business. The Consumer Privacy Notice and the business's own privacy notice cover it
The results of an account check, the masked summary of your ID, the record of your agreement, and the log of its steps (Section 2)	Dealr, with your account's security records	3 years after the check, then deleted
The one-way code made from your date of birth and name (Section 2)	Dealr, with your account's security records	3 years after the last check that used it, then deleted
Your verified identity (Section 2)	Dealr, encrypted, with your account's security records	While your account is active and for 3 years after it becomes inactive, then deleted, or sooner if you ask us to delete it (Section 8)
The details read from your ID for a request to recover your account, while the request is open	Dealr, encrypted	When the request is completed or denied, and in any case 30 days after the check
The result of the account check recorded on a request to recover your account	Dealr, with the request	3 years after the request was made, then deleted

For an account check, the images of your face and the photos of your ID follow the rows above for the face check: they are deleted when the check ends and never kept more than 1 day. No copy of your ID is filed.

Our retention rule. Biometric data is destroyed once its purpose is done. The images of your face are destroyed as soon as the check is done, and in every case within 1 day of the check. The scores we keep for some signers are destroyed within 90 days of the check. That is well before the outer limits the law sets: 3 years after your last interaction with us (Illinois), 24 months after your last interaction with us (Colorado), and one year after the purpose ends (Texas).

How it is destroyed. We permanently delete the still image and the photos of your ID from the storage area. The storage area keeps no older versions of what it holds, so a deletion is final. AWS makes its own data for the check session unavailable on the schedule above. We permanently delete the scores from our systems. Dealr never makes other copies of the images of your face.

Review. We review this schedule at least once a year to confirm that no biometric data is kept longer than this section allows. If a review ever finds biometric data that should already have been deleted, we delete it right away, and in any case within 45 days.

We follow this schedule unless a valid warrant or subpoena issued by a court requires otherwise.

The copy of your ID is a document, not biometric data under this policy, as long as no face measurements are made from it. We never run face checks on stored copies of IDs or make face measurements from them. The copy we place on your customer record, and any copy you give the business for its own records, are covered by the Consumer Privacy Notice.

---

7. How we protect it

We protect biometric data with at least the same care we use for our most sensitive confidential information, such as Social Security numbers and bank account numbers, and in line with the standard of care in our industry. In particular:

- the video travels from the camera to AWS over an encrypted connection, for a check session that can be used only once. The device uses short-lived credentials that can do nothing except start a face check;
- the still image and the photos of your ID are stored encrypted, in storage areas closed to public access;
- Dealr's servers handle the photos of your ID only while processing them, and remove temporary working files as soon as each step finishes;
- nothing is saved on the device used for the check;
- access to the AWS services and the storage area used for the check is limited to the Dealr staff who operate them; and
- our security program is audited every year (SOC 2 Type II).

Service providers. AWS and Microsoft handle the data described in this policy only under written contracts with Dealr that limit them to providing their service to us and require them to protect it at least as carefully as this section describes.

Security incidents. We keep a written plan for responding to a security incident that could affect biometric data. If a security incident ever exposes biometric data, we will notify the people affected, the business they signed with, and the government agencies the law requires, within the time the law requires.

---

8. Your questions and requests

You can contact us, using the details at the end of this policy, to:

- ask a question about this policy or the face check;
- find out what biometric data we collected about you, where it came from, why we collected it, and who received it; or
- ask us to delete information about you.

We delete the still image of your face as soon as the check is done, and we keep no other images of your face. If we kept your check's scores (Section 2), we include them when you ask what biometric data we hold, and we delete them when you ask us to delete information about you. If you ask us to delete the results of your check or the copy of your ID, we will delete them unless they must stay with your signature record to keep your signed documents verifiable, and we will tell you if that is the case. Deleting the copy of your ID also removes the copy we placed on your customer record. We keep the record of your agreement and the tamper-evident log of the check's steps as proof of your written release. They hold no images of your face and no scores. For an account check, your request covers your verified identity, the masked summaries, and the one-way codes. We delete them when you ask, except while a request to recover your account is open; we will tell you if that is the case, and delete them once it closes.

We will respond within 45 days. We will not treat you differently for asking a question or making a request.

You can also contact the business you signed with. For a transaction check, Dealr answers for the result and the record of your agreement; ask the business about the copy of your ID it keeps. For an account check, contact Dealr.

9. Who is responsible

Dealr is responsible for the biometric data collected in the face check. Dealr decides how the check works, runs it with AWS, and follows this policy. The business you are signing with chooses to use the face check for its signings and receives the result from Dealr.

Dealr is also responsible for the biometric data collected in an account check. The business you work for does not decide how the check works and does not receive your face data.

Dealr is also responsible for the biometric data collected in a transaction check. The business chooses to use it and receives the result. The copy of your ID the business keeps is the business's record.

For the rest of your transaction information, the business is responsible and Dealr handles that information on the business's behalf. The Consumer Privacy Notice explains that arrangement.

10. Washington residents: consumer health data

Washington law treats biometric data as "consumer health data." This section, together with the rest of this policy, is our consumer health data privacy policy for the face check. That law does not cover information about a person acting in an employment context, so this section applies to signers and to people completing a transaction check; we handle account checks the same way.

- **What we collect and why:** the biometric data described in Section 2, used only for the purposes in Section 3.
- **Where it comes from:** directly from you, through the device camera and the ID you present.
- **Who receives it:** AWS, as our service provider, to run the check (Section 5), and the business you are signing with or completing a transaction with, which receives the result (Section 5). We do not sell consumer health data, and we do not share it with any other third party or affiliate.
- **Your rights:** you can ask whether we collected your consumer health data and get a copy of it, get a list of any third parties and affiliates that received it, withdraw your consent, and ask us to delete it. Use the contact details at the end of this policy. We respond within 45 days. When reasonably necessary, we may take up to 45 more days, and we will tell you if we do.
- **Appeals:** if we decline to act on your request, you can appeal by replying to our decision or writing to privacy@dealr.cloud. We will respond to your appeal in writing within 45 days. If you disagree with our response to your appeal, you can contact the Washington State Attorney General.

11. Changes to this policy

We update this policy when our practices or the law change. The effective date above tells you which version you are reading. Each record of agreement notes the version of this policy that was shown. Section 3 covers any new use of biometric data.

Contact: Dealr, Inc., 1050 Eagle Dr., Loveland, CO 80537 · privacy@dealr.cloud · 720-772-7706