I am thinking to create a tool and/or word add-in for data masking/data desensitization at local computer, is there law or regulations I should know before making it available to (paid) users?

16 hours ago

I'll research this across Norwegian law, regulations, preparatory works and case law in the legal database, then summarise what applies to a local data-masking tool sold to paying users.

Used 29 tools, read 2 pages, loaded tools

I've gone through the Norwegian sources (laws, regulations, preparatory works and Supreme Court case law). A tool that runs entirely on the user's own machine keeps you out of most of data protection law as far as the documents go. The rules that actually bite are about **what you claim the tool does**, **consumer sales**, and **EU rules that are coming**.

1. Data protection (GDPR, which applies in Norway as law through personopplysningsloven § 1)

Your role depends on whether you ever touch the documents. GDPR artikkel 4 defines two roles:

- The *behandlingsansvarlig* (controller, no. 7) decides the purpose and means of the processing.
- The *databehandler* (processor, no. 8) processes data on someone else's behalf.

If the masking happens locally and nothing comes back to you, your customers are the controllers and you are neither role for their documents. That changes if you add any of these:

- Telemetry or crash reports that can capture document text.
- Cloud-based detection.
- Support where you open customer files.

These pull you into processor obligations (a data processing agreement under article 28) or full controller obligations. You *are* a controller for your own customer data: licences, payments and support emails. So you need a privacy notice (article 13) for that.

The legal duty sits with your customers, not with you. Artikkel 25 requires the *controller* to use measures such as pseudonymisation. Fortalepunkt 78 only *encourages* producers of software to build in data protection. That makes the tool a good selling point, but it does not oblige you to do anything.

The biggest legal trap is the word "anonymise."

- Artikkel 4 nr. 5 defines pseudonymisation as data that can no longer be linked to a person *without additional information*, where that information is kept separately and protected.
- Fortalepunkt 26 says pseudonymised data that can be re-linked with additional information still counts as personal data. Only truly anonymous data falls outside GDPR.
- So if your tool keeps a mapping table so masking can be reversed, the output is **pseudonymised, not anonymised**, at least for the user who holds the key. Market it accordingly.
- The EU Court of Justice nuanced this in 2025 in EDPS v SRB (C-413/23 P). The Court held that pseudonymised data must not be regarded as personal data in all cases and for every person, and that the sender's duty to inform applied before the transfer, irrespective of how the recipient sees the data. The case was decided under the parallel rules for EU institutions (Regulation 2018/1725). It supports a feature like "share a masked copy without the key," but it does not make the masked copy anonymous for your user. europa

Norwegian case law: I found no Høyesterett decision on pseudonymisation or anonymisation. The Supreme Court decisions citing personopplysningsloven deal with other issues. Datatilsynet's practice and guidance are the more relevant Norwegian sources, and they are not in this database.

2. Selling to consumers

If private individuals can buy the tool, these Norwegian rules are mandatory. If you sell only to businesses, contract freedom largely applies and your licence terms do the work.

- **Digitalytelsesloven** covers paid digital content and services to consumers (§ 1). The preparatory works list computer programs and applications as examples (Prop. 66 LS (2021–2022), comment on § 1). Key points:
  - You cannot contract out of it to the consumer's detriment (§ 3).
  - § 8 requires the product to match what the consumer may expect, *including your own marketing claims*. Overstating detection accuracy can therefore make the product legally defective.
  - § 8 also requires the product to be free of third parties' rights, such as IP. Check the licences of your open-source libraries and detection models.
  - § 9 requires you to inform consumers about and deliver necessary updates, including security updates.
- **Withdrawal right:** consumers normally get 14 days to withdraw. For downloaded software, the right lapses only if all of these are met (angrerettloven § 22 bokstav n):
  - The consumer has expressly agreed that delivery starts early.
  - The consumer has acknowledged that this ends the withdrawal right.
  - You have sent the confirmation the law requires.

  Build this into your checkout.
- **Marketing:** markedsføringsloven § 7 bans misleading claims about a product's main characteristics, results or fitness for purpose. "GDPR-compliant," "100 % anonymised" or "catches all personal data" are risky claims. The section has an amendment pending, with no in-force date yet.
- **Website information:** ehandelsloven § 8 requires your name, address, email, organisation number and VAT status to be easy to find.

3. Liability if the tool misses something

The realistic scenario is that a customer relies on the masking, an unmasked personal data item slips through, and the customer suffers a data breach.

- Norway's produktansvarsloven § 1-2 defines "product" as goods and movables ("varer og løsøre"). Whether standalone software fits that wording is not settled in what I found.
- Today your main exposure is therefore **contractual**. Clear terms help:
  - The tool is an aid and the user must review the output.
  - A limitation of liability, within the mandatory consumer rules above.
- The EU's new Product Liability Directive (2024/2853) has an EU compliance date of 9 December 2026. It is **not yet part of Norwegian law** and is under EEA scrutiny (status). I couldn't open its text here, so check on EUR-Lex how it treats software before relying on it.

4. EU rules on the horizon (not yet Norwegian law)

These were adopted in the EU but not yet incorporated into the EEA Agreement as of today. They may still apply directly if you sell into EU countries. I couldn't open their texts here, so their detailed obligations are unverified.

- **Cyber Resilience Act (2024/2847)** sets horizontal cybersecurity requirements for "products with digital elements." The EU compliance date is 11 December 2027 (EEA status). This is the one most likely to affect a commercial desktop tool or add-in. Plan for vulnerability handling and a defined security-update period from the start.
- **AI Act (2024/1689)**: EU compliance date 2 August 2026, not EEA-incorporated (status). It is only relevant if you use machine-learning models (for example name or entity recognition) for detection. Check whether any obligations attach.

5. Accessibility

Likestillings- og diskrimineringsloven § 18 requires private businesses to make their main user-facing ICT solutions universally designed. That covers at least your website and webshop, possibly the tool's interface. There is an exception for disproportionate burden, where size and cost count.

What this means for your design

- Keep processing fully local, and make telemetry and crash reporting opt-in and free of document content. This keeps you out of the processor role.
- Call reversible masking "pseudonymisation." Use "anonymisation" only for irreversible modes, and even then avoid absolute claims.
- Let users keep or discard the key themselves, so they can share a masked copy without it.
- Use cautious, accurate marketing and terms that say the user must review the output.
- Set up a consumer checkout that meets angrerettloven § 22 n, and commit to a security-update policy.
- Separately (contract, not law): Microsoft's add-in store terms and your dependencies' open-source licences.

I'm not a lawyer, and this is information from the retrieved sources, not legal advice. Before launch, it's worth having a lawyer review your licence terms and marketing claims. You can find one via Advokatenhjelperdeg, and Datatilsynet's guidance service can answer general questions on the data protection side.

Sources:

- Personopplysningsloven § 1; GDPR artikkel 4; GDPR artikkel 25; GDPR fortalepunkt 26 and 78
- Digitalytelsesloven §§ 1, 3, 8, 9; Prop. 66 LS (2021–2022)
- Angrerettloven § 22; Markedsføringsloven § 7; Ehandelsloven § 8
- Produktansvarsloven § 1-2; Likestillings- og diskrimineringsloven § 18
- Cyber Resilience Act; Product Liability Directive 2024; AI Act; EEA status at efta.int
- CJEU, C-413/23 P EDPS v SRB (press release, curia.europa.eu)

Ask Claude your own question