ACE POS Solutions Ltd.

GDPR Tips for North American Small Businesses

www.acepos-solutions.com

GDPR - How to get started

1) Do a privacy audit

Use the 2 following checklists to list all places where you keep and collect personal data

2) Existing EU data?

Do you have existing EU data? If you do, can you segment it separately? Consult a legal advisor to handle existing & new EU data.

3) What is your basis?

Determine what lawful basis you have to collect personal data. Consent? Contract? Legal Obligation? Legitimate Interests?

4) Delete unwanted data & review existing

Delete anything unnecessary or unlawful and consider asking data subjects to opt-in again.

5) Update policies

Update privacy policy, terms of service, employee contracts and supplier contracts. Post privacy policy and terms of service on your web site. Email updated privacy policy to subscribers.

6) Revise processes

Add explicit, positive, documented consent wherever possible (e.g. add opt-in checkboxes to your web site, your forms, etc.). Review the cookie policy on your web site. Review supplier privacy practices.

7) Review 3rd party processors & sign DPAs

Sign all required Data Processing Agreements (DPA) with processors (Google Analytics, MailChimp, etc.)

8) Review data security

Review all data collection, handling and security with staff. Make you restrict access to your back-ups to minimize risk.

Knowing is half the battle

To meet legal requirements and deal with potential data breaches, you need to know WHERE and HOW you are collecting Personally Identifiable Information (PII). Make a spreadsheet to log your answers below:

- [ ] **Where do we store existing PII in the business?** (digital, hardcopies, etc.)
- [ ] **Where do we collect new PII in the business?** (physical store, Shopify store, etc.)
- [ ] **Do we collect PII from any European citizens or residents?**
- [ ] **What are we using to collect PII?** (website form, POS, MailChimp, Google Analytics, third-party source, etc.)
- [ ] **What type of PII are we collecting?** (signatures, names, emails, postal codes, IP addresses, etc.)
- [ ] **What is our reason for collecting this PII?** (Consent, Contract, Legal Obligation, Legitimate Interest)
- [ ] **Where is the PII stored?** (company server, employee computers/mobiles, own cloud server, supplier servers)
- [ ] **Who has access to this PII?**
- [ ] **What security is used to protect this PII?**
- [ ] **Is this data really needed for the business?**
- [ ] **How long are we legally allowed to keep this PII?**

Where is my data?

- [ ] Existing files, documents or images that contain PII (digital, paper, audio) including back-ups
- [ ] Existing company and staff devices that hold PII
- [ ] Existing third-party suppliers that hold PII
- [ ] Signature capture forms and devices (digital, paper)
- [ ] Telecommunication systems (call records, voicemails, chat, SMS)
- [ ] File, email and web hosting and backend infrastructure
- [ ] Accounting systems including payroll services
- [ ] Payment handling services and tools
- [ ] Marketing tools including analytical services (advertising, web analytical services, review services, surveys, email campaigns, etc.)
- [ ] Social media accounts, messages, chats
- [ ] Sales tools (CRM, calendars, webinars, etc.)
- [ ] Recording services (heatmaps, CCTV)
- [ ] Integrations that pass PII (Zapier)
- [ ] Remote access tools
- [ ] Ticketing systems for support, training, development, project management
- [ ] Internal chat / tasking software (Slack, Trello)