🔐 Employee Guide to Data Protection (GDPR & CCPA)

1. Understand Personal Data

Personal data = Any information that identifies a person (e.g., name, email, ID, IP address, location, etc.).
Sensitive personal data = religion, gender, political direction, military status, health status, etc.

---

2. Follow These Core Principles

✅ Only collect what's needed

- Don't ask for or store more data than required for your task.

✅ Use it only for its intended purpose

- Use personal data only for the reason it was collected.
- Don't reuse data for other purposes without permission.

✅ Keep data accurate

- Check data for accuracy and update it when needed.

✅ Limit access

- Only authorized people should access personal data.
- Don't share data unless necessary and permitted.

✅ Store it securely

- Use strong passwords and approved systems.
- Never save personal data on unsecured devices or platforms.

✅ Delete when no longer needed

- Follow retention policies.
- Don't keep personal data longer than necessary.

---

3. Use of Emrich-IPR Email Addresses:

- The IPR email address may only be used for business purposes.
- All emails sent or received via this account are archived centrally in order to comply with the "Principles for the proper keeping and storage of books, records and documents in electronic form and for data access" (GoDB) issued by the German Federal Ministry of Finance in 2014.

- Do not grant third parties (including family members) access to the emails.
- Automatic forwarding of company emails to an email address outside the company is not permitted for data protection reasons.
- Business emails may only be processed on end devices that have adequate password protection.

---

4. Respect Rights of Individuals

Right	GDPR	CCPA
Access	✅ Individuals can see their data	✅ Same
Correction	✅ They can fix wrong data	❌ Not required
Deletion	✅ "Right to be forgotten"	✅ "Right to delete"
Data Portability	✅ Must provide data in a usable format	❌ Not required
Opt-out of selling	❌	✅ Consumers can stop sale of their data

---

5. What You Must Not Do

- ❌ Don’t send personal data via unsecured emails.
- ❌ Don’t leave printed data unattended.
- ❌ Don’t discuss personal data in public areas.
- ❌ Don’t upload personal data to unapproved platforms.

---

6. Report Incidents Immediately

If you lose data, suspect a breach, or make a mistake involving personal data:

- **Report it right away** to your Supervisor or IT/security team.

---

7. Need Help?

When in doubt, ask your:

- **Supervisor: Claudia Haessler (chaessler@emrich-ipr.com)**

🛡️ Final Tip

Treat all personal data as if it were your own.