GDPR Compliance Guide

Document Number: COMP-DP-001 **Effective Date:** May 25, 2018 **Last Updated:** January 15, 2024 **Owner:** Legal & Compliance **Applies To:** All employees handling EU personal data

Overview

The General Data Protection Regulation (GDPR) is the European Union's data protection law that governs how organizations collect, process, and store personal data of EU residents. This guide explains NovaTech's GDPR compliance requirements and your responsibilities.

What is GDPR?

GDPR is a comprehensive data protection regulation that: - Applies to any organization processing EU residents' data - Gives individuals control over their personal data - Requires transparency about data use - Imposes significant penalties for non-compliance

Scope

GDPR applies when NovaTech: - Has EU-based customers or users - Has EU-based employees - Processes data of EU residents (regardless of location) - Offers services to the EU market

Key Concepts

Personal Data

Personal data is any information relating to an identified or identifiable person: - Name, email address - IP addresses - Location data - Online identifiers (cookies, device IDs) - Employment information - Any data that could identify someone

Sensitive Personal Data (Special Categories)

Requires extra protection: - Racial or ethnic origin - Political opinions - Religious beliefs - Trade union membership - Health data - Sexual orientation - Biometric data - Genetic data

Data Subject

The individual whose personal data is being processed.

Data Controller

The organization that determines the purposes and means of processing. **NovaTech is a data controller** for customer and employee data.

Data Processor

The organization that processes data on behalf of a controller. **NovaTech is a data processor** when processing customer's end-user data.

GDPR Principles

All data processing must follow these principles:

1. Lawfulness, Fairness, Transparency

- Have a legal basis for processing
- Process data fairly
- Be transparent about what you do with data

2. Purpose Limitation

- Collect data for specific, explicit purposes
- Don't use data for incompatible purposes

3. Data Minimization

- Collect only what you need
- Don't collect "just in case"

4. Accuracy

- Keep data accurate and up-to-date
- Correct inaccuracies promptly

5. Storage Limitation

- Don't keep data longer than necessary
- Delete or anonymize when no longer needed

6. Integrity and Confidentiality

- Keep data secure
- Protect against unauthorized access

7. Accountability

- Document compliance efforts
- Be able to demonstrate compliance

Legal Bases for Processing

You need a legal basis to process personal data:

Legal Basis	When It Applies
Consent	Individual has given clear consent
Contract	Necessary to fulfill a contract
Legal obligation	Required by law
Vital interests	Protecting someone's life
Public interest	Performing a public task
Legitimate interests	Necessary for legitimate business interests (balanced against individual rights)

At NovaTech

Data Type	Typical Legal Basis
Customer account data	Contract
Employee data	Contract, legal obligation
Marketing (opted-in)	Consent
Product analytics	Legitimate interests
Security logs	Legitimate interests

Individual Rights

Data subjects have the following rights:

Right to Be Informed

- Privacy notices
- Clear explanation of data use

Right of Access (Subject Access Request)

- Get a copy of their data
- Know how it's used
- Response within 30 days

Right to Rectification

- Correct inaccurate data
- Complete incomplete data

Right to Erasure ("Right to be Forgotten")

- Delete their data in certain circumstances
- Not absolute (some exceptions apply)

Right to Restrict Processing

- Limit how their data is used

Right to Data Portability

- Receive data in machine-readable format
- Transfer to another service

Right to Object

- Object to processing based on legitimate interests
- Object to direct marketing (absolute right)

Rights Related to Automated Decision-Making

- Not be subject to purely automated decisions
- Obtain human intervention

Handling Data Subject Requests

If You Receive a Request

1. **Don't respond yourself** - Forward to privacy@novatech.com immediately
2. **Document receipt** - Note date and channel received
3. **Verify identity** - The Privacy team will verify the requestor
4. **Deadline:** 30 days from receipt (most requests)

What the Privacy Team Does

1. Verify the request is valid
2. Identify relevant data
3. Consult with relevant teams
4. Fulfill or explain why it can't be fulfilled
5. Respond within deadline

Data Protection by Design

Build privacy into products and processes:

Design Phase

- Conduct Data Protection Impact Assessment (DPIA) for high-risk processing
- Minimize data collection
- Plan for data subject rights
- Build in security controls

Development

- Use pseudonymization where possible
- Implement access controls
- Log access for audit purposes
- Test security

Operation

- Regular access reviews
- Monitor for breaches
- Maintain documentation
- Update as needed

Data Breach Notification

What is a Breach?

Security incident affecting personal data: - Unauthorized access - Data loss - Accidental disclosure - System compromise affecting personal data

Reporting a Suspected Breach

Report immediately to security@novatech.com: - What happened - What data may be affected - When it was discovered - Any immediate actions taken

Regulatory Notification

If a breach is likely to result in risk to individuals: - Notify supervisory authority within **72 hours** - The Privacy team handles this notification

Individual Notification

If a breach is likely to result in high risk: - Notify affected individuals without undue delay - The Privacy team coordinates notification

International Data Transfers

Transferring personal data outside the EU requires safeguards:

Approved Mechanisms

Mechanism	Description
Adequacy decision	EU approved the destination country
Standard Contractual Clauses (SCCs)	EU-approved contract terms
Binding Corporate Rules	Approved intra-group transfers
Derogations	Specific exceptions (limited use)

NovaTech Approach

- EU data primarily processed in EU data centers
- US transfers use SCCs and supplementary measures
- Data Processing Agreements include transfer mechanisms

Vendor Management

When working with vendors who process personal data:

Requirements

- Data Processing Agreement (DPA) required
- Assess vendor security practices
- Ensure GDPR compliance
- Maintain records of processing

Process

1. Identify vendors processing personal data
2. Conduct due diligence
3. Execute DPA before sharing data
4. Monitor ongoing compliance

Contact privacy@novatech.com for vendor assessments.

Employee Responsibilities

All Employees

- Complete annual GDPR training
- Handle personal data carefully
- Report potential breaches immediately
- Respect data subject rights
- Only access data you need

Managers

- Ensure team compliance
- Include privacy in project planning
- Escalate concerns appropriately

Specific Roles

Role	Additional Responsibilities
Engineering	Privacy by design, security controls

Role	Additional Responsibilities
Product	Data minimization, consent UX
Customer Success	Handle DSRs appropriately
Marketing	Consent management, opt-outs
HR	Employee data protection

Documentation

What We Document

- Processing activities (Records of Processing)
- Legal bases for processing
- Data retention schedules
- Data Protection Impact Assessments
- Breach incidents
- Data subject requests

Where to Find It

- Privacy documentation: Legal > Privacy in Notion
- Privacy notices: novatech.com/privacy
- Internal policies: Compliance > Data Privacy in Notion

Training

Required Training

All employees must complete: - **GDPR Fundamentals** - Annual (Workday Learning) - **Role-specific training** - As assigned

Additional Resources

- Privacy Office Hours - Monthly (see calendar)
- #privacy-questions Slack channel
- Privacy documentation in Notion

Getting Help

Privacy Team

- **Email:** privacy@novatech.com

- **Slack:** #privacy-questions
- **DPO:** dpo@novatech.com (for formal matters)

When to Contact

- Questions about handling personal data
- New project involving personal data
- Potential data breach
- Vendor engaging with personal data
- Data subject request received

Consequences of Non-Compliance

For NovaTech

- Fines up to €20 million or 4% of global revenue
- Reputation damage
- Legal action from individuals
- Regulatory investigation

For Employees

- Disciplinary action for policy violations
- Personal liability in extreme cases

Summary Checklist

Before handling personal data, ask:

☐ Do I have a legal basis for this processing?
☐ Am I only collecting necessary data?
☐ Is the data stored securely?
☐ Do I have the right access?
☐ Could a data subject exercise their rights?
☐ Is there a retention schedule?
☐ If sharing externally, is there a DPA?

Contact

For GDPR questions: - **Privacy Team:** privacy@novatech.com - **DPO:** dpo@novatech.com - **Slack:** #privacy-questions

Related Documents: Data Retention Policy (COMP-DP-005), Data Subject Request Procedures (COMP-DP-010), Privacy Impact Assessment Guide (COMP-DP-015), Data Breach Procedures (COMP-DP-020)