GDPR Compliance Guide

Document ID: COM-IR-010 **Effective Date:** January 1, 2024 **Last Updated:** February 2024 **Owner:** Legal & Compliance **Classification:** Internal

---

Overview

The General Data Protection Regulation (GDPR) applies to NovaTech when we process personal data of individuals in the European Union/European Economic Area (EU/EEA). This guide outlines our compliance approach.

When GDPR Applies

Applicability

GDPR applies to NovaTech when: - Processing data of EU/EEA residents - Offering products/services to EU/EEA - Monitoring behavior of EU/EEA individuals - Having employees in EU/EEA

Our Role

As a Data Controller: When we collect and process data for our own purposes (e.g., employee data, marketing)

As a Data Processor: When we process data on behalf of customers (e.g., customer data in our products)

Key Principles

Lawfulness, Fairness, Transparency

- Process data with a legal basis
- Be clear about what we do with data
- Don't deceive individuals

Purpose Limitation

- Collect for specified, explicit purposes
- Don't process for incompatible purposes
- Document purposes clearly

Data Minimization

- Collect only what's necessary
- Don't accumulate "just in case"
- Regularly review data holdings

Accuracy

- Keep personal data accurate
- Update when necessary
- Allow corrections

Storage Limitation

- Keep only as long as needed
- Follow retention schedules
- Delete when purpose is fulfilled

Integrity and Confidentiality

- Ensure appropriate security
- Protect against unauthorized access
- Protect against accidental loss

Accountability

- Be able to demonstrate compliance
- Document decisions and measures
- Maintain appropriate records

Legal Bases for Processing

Available Bases

Legal Basis	When to Use	Example
Consent	Freely given, specific, informed	Marketing emails
Contract	Necessary for contract performance	Customer service delivery
Legal Obligation	Required by law	Tax reporting
Vital Interests	Protecting life	Emergency contact
Public Interest	Official authority	N/A for NovaTech
Legitimate Interest	Business need, balanced with rights	Security monitoring

Common NovaTech Uses

Processing Activity	Legal Basis
Employee HR data	Contract, Legal Obligation
Customer account data	Contract
Marketing emails	Consent
Security monitoring	Legitimate Interest
Product analytics	Legitimate Interest (with safeguards)

Individual Rights

Right to be Informed

What: Clear information about data processing **How we comply:** - Privacy notices on website - Employee privacy policy - Customer data processing terms

Right of Access (Subject Access Request)

What: Copy of personal data we hold **How we comply:** - Process within 30 days - Provide data in portable format - Verify identity before disclosing

Right to Rectification

What: Correction of inaccurate data **How we comply:** - Self-service where possible - Process requests promptly - Update all systems

Right to Erasure ("Right to be Forgotten")

What: Deletion of personal data **When it applies:** - Consent withdrawn - No longer necessary - Unlawful processing **Exceptions:** - Legal obligations - Legal claims - Public interest

Right to Restrict Processing

What: Limit how we use data **When it applies:** - Accuracy contested - Processing unlawful - No longer needed but required for legal claims

Right to Data Portability

What: Receive data in machine-readable format **When it applies:** - Processing based on consent or contract - Automated processing

Right to Object

What: Object to processing **When it applies:** - Legitimate interest processing - Direct marketing (absolute right)

Rights Related to Automated Decision-Making

What: Not be subject to solely automated decisions with significant effects **How we comply:** - Human review for significant decisions - Right to explanation - Right to contest

---

Handling Data Subject Requests

Process

1. **Receive request:** Any channel (email, form, verbal)
2. **Verify identity:** Ensure requester is the data subject
3. **Log request:** Record in DSR tracker
4. **Respond within 30 days** (extendable to 90 for complex requests)
5. **Document response:** Keep record of action taken

Where to Send Requests

- Customers: privacy@novatech.com
- Employees: hr@novatech.com
- Website visitors: privacy@novatech.com

Response Requirements

- Free of charge (except for manifestly unfounded/excessive)
- In writing or electronically
- Clear and plain language
- Provide reason if refusing

Data Protection Impact Assessments (DPIA)

When Required

DPIA required for: - Systematic, extensive profiling - Large-scale processing of special categories - Systematic monitoring of public areas - New technologies with high risk - Cross-referencing datasets

DPIA Process

1. Describe the processing
2. Assess necessity and proportionality
3. Identify and assess risks
4. Identify measures to mitigate risks
5. Document and review
6. Consult DPO if high residual risk

Template

Use DPIA template in Confluence: Legal → Privacy → DPIA Template

---

International Data Transfers

Allowed Transfers

Data can be transferred outside EU/EEA when: - Adequacy decision (e.g., UK, Canada, Japan) - Standard Contractual Clauses (SCCs) - Binding Corporate Rules - Explicit consent (limited circumstances)

US Transfers

NovaTech uses: - Standard Contractual Clauses - Data Processing Agreements - Supplementary technical measures

Customer Data

- DPA includes GDPR-compliant transfer mechanisms
- Sub-processor list maintained
- Customer notification for sub-processor changes

Data Breach Notification

What's a Breach

Personal data breach includes: - Unauthorized access - Data loss - Destruction of data - Disclosure to wrong party

Notification Requirements

To Supervisory Authority: - Within 72 hours of awareness - Unless unlikely to result in risk

To Individuals: - Without undue delay - When likely high risk to rights and freedoms

Breach Response Process

1. Contain and assess the breach
2. Notify Security team immediately
3. Document the breach
4. Assess risk to individuals

5. Notify authority if required
6. Notify individuals if required
7. Document response and lessons learned

See: Incident Response Plan (IT-SEC-010)

Vendor Management

Data Processing Agreements

Required for all processors handling EU personal data: - Processing only on documented instructions - Confidentiality obligations - Security measures - Sub-processor restrictions - Assistance with rights requests - Audit rights - Deletion at end of contract

Vendor Assessment

Before engaging vendor with EU data: 1. Data protection questionnaire 2. Review of security measures 3. DPA execution 4. Documented approval 5. Ongoing monitoring

---

Employee Responsibilities

All Employees

- Complete GDPR training
- Handle personal data appropriately
- Report potential breaches immediately
- Follow data handling procedures
- Respect individual rights

Managers

- Ensure team compliance
- Support training completion
- Escalate concerns

Specific Roles

Product team: Privacy by design **Engineering:** Technical safeguards **Sales/Marketing:** Consent management **HR:** Employee data protection **Customer Success:** Rights request handling

---

Privacy by Design

Principles

Build privacy into products/processes: 1. Proactive, not reactive 2. Privacy as the default 3. Privacy embedded in design 4. Full functionality (not privacy vs. features) 5. End-to-end security 6. Visibility and transparency 7. Respect for user privacy

Implementation

New Products: - DPIA for new features - Privacy review in development - Data minimization in design - Consent mechanisms

Existing Products: - Regular privacy reviews - Data inventory updates - Enhancement for compliance

---

Training Requirements

Required Training

Training	Audience	Frequency
GDPR Basics	All employees	Annual
Advanced GDPR	Privacy team, legal	Annual
Role-specific	Varies	As needed

Training Topics

- GDPR overview
- Individual rights
- Data handling

- Breach reporting
- Role-specific requirements

Documentation

Required Records

- Records of processing activities (ROPA)
- DPIAs (where conducted)
- Consent records
- Rights request records
- Breach records
- Training records

Where Maintained

- Legal → Privacy folder in Confluence
- ROPA in compliance tool
- Training records in Workday

Roles

Data Protection Officer (DPO)

- Contact: dpo@novatech.com
- Independence in role
- Reports to Legal and Board

DPO Responsibilities

- Monitor compliance
- Advise on privacy matters
- Point of contact for authorities
- Point of contact for individuals

When to Contact DPO

- New processing activities
- Potential breaches
- DPIA consultations
- Complaints
- Authority inquiries

Compliance Monitoring

Regular Activities

- Quarterly privacy reviews
- Annual ROPA updates
- Periodic DPIAs
- Training tracking
- Vendor assessments

Audits

- Internal privacy audits
- External audits (SOC 2 includes privacy)
- Authority audits (if requested)

Contacts

- **DPO:** dpo@novatech.com
- **Privacy Team:** privacy@novatech.com
- **Legal:** legal@novatech.com
- **HR (employees):** hr@novatech.com

Related Documents: Privacy Policy Internal (COM-DP-010), Data Retention Policy (COM-DP-005), Data Classification Policy (IT-SEC-005)