NAVEX™

Checklist

NAVEX IRM GDPR Compliance Checklist

GDPR compliance. From quick answers to a checklist for getting started.

What is GDPR?

The European Union (EU) General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and is designed to protect the data privacy of EU citizens.

Where does it apply?

GDPR applies to all member states in the EU.

Who falls under GDPR?

Any company in the world with employees or customers with citizenship in an EU country must comply with GDPR.

When does it take effect?

The GDPR regulation went into effect on May 25, 2018.

Why GDPR?

There's a growing call around the world for individual privacy and data protection. It's led countries from Australia and the United States to the EU and Asia-Pacific to pass national privacy regulations like GDPR.

The following GDPR Checklist has been brought to you by NAVEX IRM, which offers a comprehensive, integrated approach to complying with GDPR. To learn more, contact us at +1 866 297 0224 or email info@navex.com.

GDPR Checklist

Use this checklist to get started on GDPR compliance.

Inventory your data

Think of all the ways you collect, store, and distribute people's privacy information and document accordingly.

- [ ] Catalog assets that contain privacy data
- [ ] Identify and document how that data is collected
- [ ] Document where and how data is stored and backed up
- [ ] Identify person(s) with access to the data and how permissions are handled

Perform risk assessments

GDPR will impact all aspects of the business. Conducting risk assessments is essential.

- [ ] Identify risks to the company and their business criticality
- [ ] Assess all business functions, not just IT
- [ ] Perform third-party risk assessments on their privacy policies and procedures

Review policies and procedures

Creating new controls impacts policies. In this step, review your company policies and procedures.

- [ ] Review all company policies and procedures against GDPR requirements
- [ ] Update existing policies and procedures in accordance with GDPR requirements
- [ ] Create new policies and procedures if determined from gap analysis
- [ ] Link policies to procedures and controls to prove compliance

Test run your GDPR program

Create and run an internal test using GDPR's requirement to grant a person's right to erase their personal information.

- [ ] Identify the type of personal information that needs to be deleted
- [ ] Identify the assets that house that type of information. Don't forget backups
- [ ] Perform deletion of personal information and document the action
- [ ] Confirm deletion through company, backup and vendor systems
- [ ] Document the actions required and taken, citing controls and policies
- [ ] Make any adjustments required to comply

Document GDPR activities

Be ready for a GDPR compliance audit by documenting your GDPR compliance activities.

- [ ] Document all privacy requests and actions taken to satisfy those requests
- [ ] Create audit trails in the event you undergo a GDPR audit
- [ ] Generate any reports required for GDPR compliance

WWW.NAVEX.COM | info@navex.com | +1 866 297 0224