ZALARIS

Guide to GDPR Compliance

Ensure your company is on – and stays on – the right path

For HR & Human Capital Management

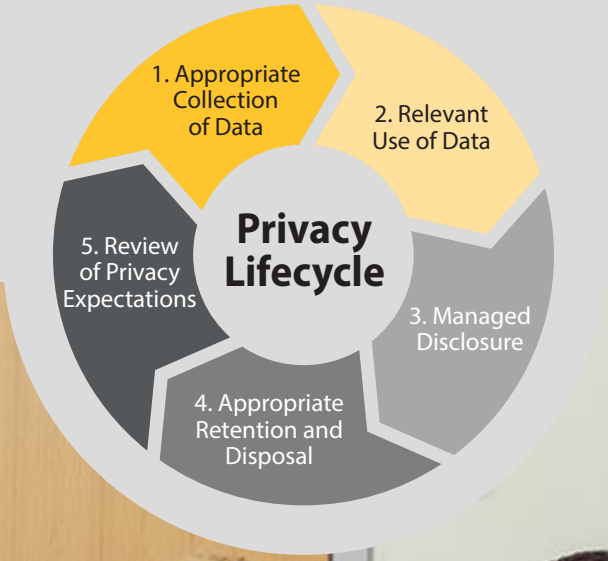
SAP Gold Partner

Guide to GDPR Compliance

Quick Links

GDPR Up Close and Personal in HR

Protecting the right to privacy is not new. What constitutes personal data, however, has expanded with the General Data Protection Regulation, and the rights of data subjects are broader. These changes in scope are among the new considerations critical from a human resources standpoint. The new regulation also unifies aspects of existing Data Protection Act regulations. European Union member states now have more consistent standards, although individual countries can still impose their own unique data privacy conditions — all of which warrant increasingly tighter controls and management.



The privacy lifecycle, as illustrated here, deserves renewed scrutiny, assessment and action from an HR perspective. Although employers have inherent requirements associated with data essential to recruiting, hiring and performance management, relevant use must still be justifiable. There's no margin for error now, especially in light of new GDPR penalties enforceable as of May 2018.

Zalaris is a partner that knows the HR responsibilities, accountabilities and measures necessary for GDPR compliance. The challenges are much greater, given the security demands and complexities of the digital era and the "right to be forgotten," balanced with your needs as an employer. We are an ideal partner in developing and maintaining privacy solutions "by design," as GDPR mandates. Our experience, processes and solutions make a profound difference each step of the way in your data journey.

Considerations and Consequences

GDPR represents a mix of old and new in an ambitious goal for cross-border alignments. Considerations range from continued existing legislation that should already be on your agenda to clarifications and enhanced statements on certain privacy principles – as well as clearly defined new rules requiring careful planning to apply in practice. As you contemplate these issues and consequences, you may hear divergent views ranging from *"The GDPR doesn't really represent big news for us and won't significantly alter how we run our business"* to *"The GDPR is a paradigm shift and has our Board's attention as the largest of our current change programs!"* Whatever view you adopt, the following realities must be faced:

10 GDPR Realities

1 More Control to Individuals
Employees receive clear information about how their personal information is processed and protected. They have the right to review, correct and limit the storage time of their data.

2 One Supervisory Authority
Organizations need only report to one lead supervisory authority, which will coordinate with other 'concerned' supervisory authorities when necessary.

3 Personal Data Inventory
Overview of personal data maintained "in-house" to show where data is held and processed, including all systems and countries.

4 Risk-based Approach Advocated
Controllers of data should first identify and address related activities that are at the highest risk of compromise, then do the same for those deemed lower risk.

5 Privacy by Design
All systems should inherently address privacy concerns – literally by design. From the onset, personal data must be appropriately accessed and used in accordance with GDPR standards/guidance.

6 Processor and Controller Roles
Controllers and processors are subject to GDPR scrutiny and responsibilities from different perspectives. Transparency is of critical importance.

7 Accountability Factors
You not only must comply with GDPR mandates but also demonstrate compliance while ensuring new projects/processes include privacy impact assessments.

8 Data Protection Officer Role
Your organization may need to appoint a "DPO," which is a central position responsible for reviewing and reporting to highest levels about data protection.

9 Reporting Suspected Breaches
Personal data breaches must be reported within 72 hours (unless a delay is justified) to corresponding supervisory authority as well as affected data subjects.

10 Fines for Non-Compliance
Sanctions can be imposed up to 4% of annual revenue or €20 million, and affected individuals are also able to sue for material and non-material damages.

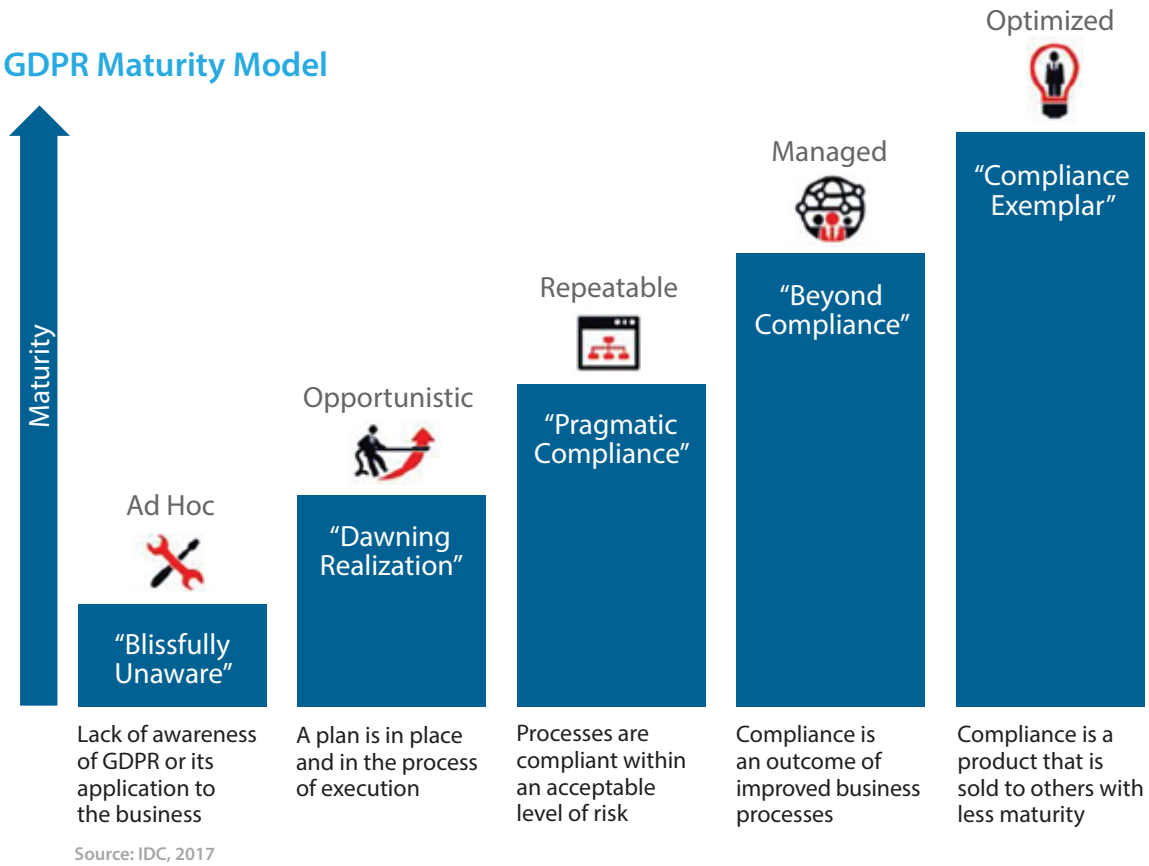
The Deep Value of GDPR Initiatives

With all the complexity that can be associated with meeting GDPR requirements, it's easy to lose sight of the many positives that compliance initiatives enable. We speak from extensive specific experience in the world of HR, HCM and payroll functions...the people side of every enterprise, where Zalaris delivers its core value. Our business model encompasses the unique *advantages* that GDPR now mandates.

Protecting personal data has always been essential to our success, and the types of security measures, processes and structure we deliver further attests to why we should be your partner in the HR GDPR journey. Zalaris enables alignment across organizations through system-supported best practice processes to manage your HR data effectively, including support for cross-border transfers.

As you can see from the IDC chart below, the GDPR journey generally fits into a series of categories relative to a company's corresponding level of maturity. The spectrum begins with "Blissfully Unaware," which certainly won't serve as an effective defense for non-compliance, and concludes with our territory, "Compliance Exemplar." We will help you move *beyond compliance* for remarkable overall business benefits. This is where Zalaris thrives – helping companies achieve excellence from all perspectives, including leadership, business performance and operations as well as the satisfaction of your people.

The Zalaris toolset will help clarify real maturity in different parts of the organization, relating to various solutions and connected processes. Zalaris' involvement in GDPR projects across a large international client base will help in clarifying requirements while further supporting GDPR best practices.



Source: IDC, 2017

Proactive Engagement Essential to Achieving & Maintaining Compliance

Cooperation and joint alignment are vital to ensuring full protection relative to GDPR stipulations. Controllers and processors of data must work together, especially in an environment with outsourced service providers. The range of variations and interconnections can be extraordinary, requiring a case-dependent analysis and custom action plan.

Controller Responsibilities

Determines the purposes and means of the processing of personal data.

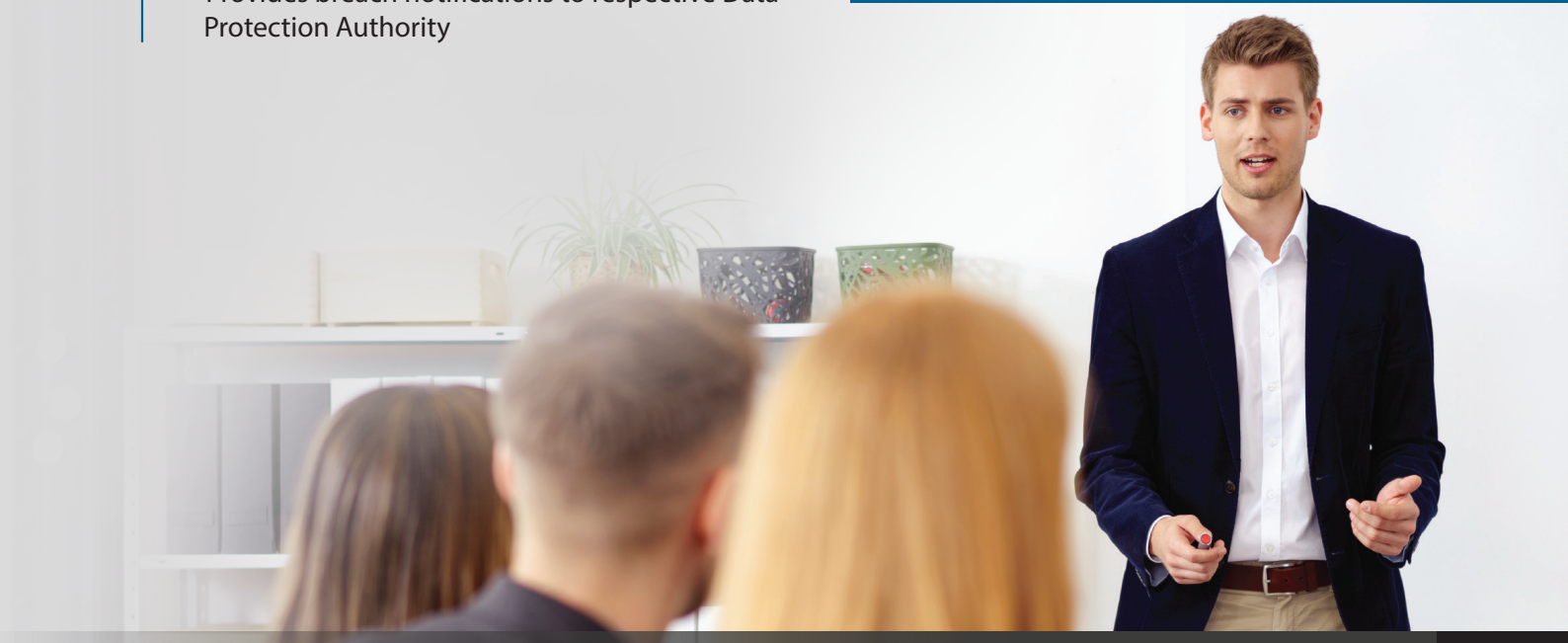
- Decides to collect the personal data in the first place (and the legal basis for doing so) for each employee and respective data-use purposes
- Determines whether subject access and other individuals' rights apply while respecting the law
- Settles on how long to retain data for specific purpose in accordance with regulations
- Conducts Data Protection Impact Assessment (DPIA) and consulting prior to processing
- Implements appropriate technical and organizational measures
- Only selects processors that provide sufficient guarantees of their ability to implement technical and organizational compliance measures
- Establishes contract with processor, containing provisions regarding the tasks and responsibilities of the processor and related governance
- Provides breach notifications to respective Data Protection Authority

Processor Responsibilities

Processes personal data on behalf of controller based on contractual obligations.

- Reviews contract and instructions and ensures relevance and clarity
- Maintains records of all categories of personal data carried out on behalf of the controller
- Provides appropriate technical and organizational measures supporting compliance
- Demonstrates accountability in specified areas of contractual obligation
- Deletes or returns data to the controller upon completion of processing
- Submits to specific terms and conditions for engaging sub-processors
- Notifies the controller in case of breaches

Take a collaborative approach to "controller" and "processor" roles, including clear communications, structured workflow and standardized processes.



Keys to Successfully Managing Personal Data

What it takes to successfully manage personal data in the GDPR era comes down to many factors. The spectrum is summarized in the chart below, representing the primary categories that must be addressed at a high level.

A highly structured approach must be embraced to successfully navigate the detailed processes, digital and paper record trails as well as various steps associated within each stage of the data journey. From the time you hire and throughout each employee's tenure — and afterward — the responsibilities are more daunting than ever.

It begins with the right design, migration strategy, interfaces and storage matters, addressing data management at the time of a new hire's onboarding, departure or retirement. Transparency, access and rectification are also part of the equation.

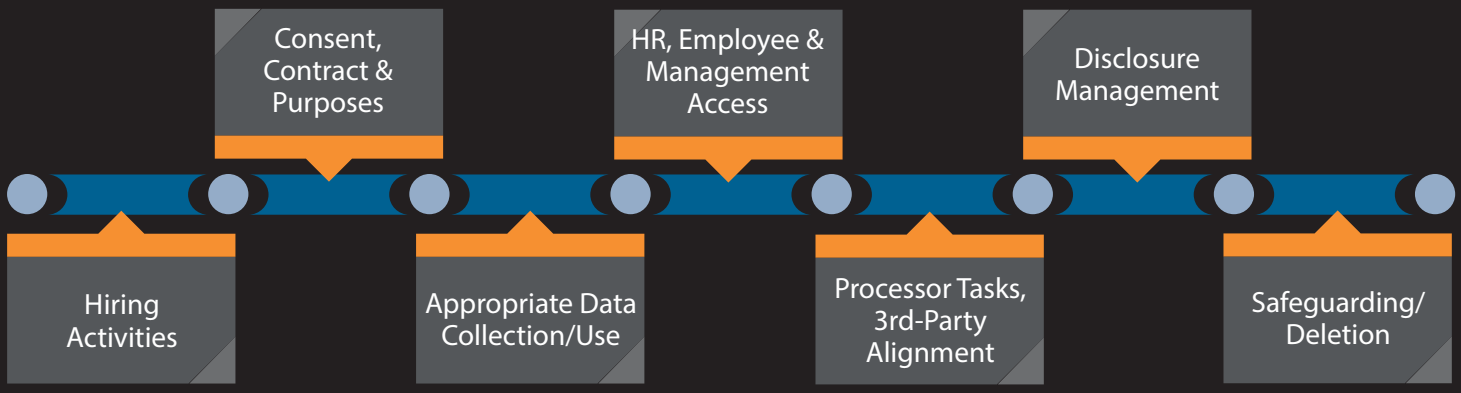
Will you have the efficiencies of an employee-oriented shared-services model? How are you adapting information security in HCM and CRM solutions in addition to daily workflow, as well as the role of analytics across both structured and unstructured data? Routine forms and other everyday online employee interactions suddenly become risk points. Gap identification towards the new standard is an essential starting point.

Assess Where You Are — and Need to Be

The biggest mistake that likely can be made relative to GDPR is to underestimate what's involved to ensure compliance. Zalaris provides expert guidance relative to all aspects of the data journey, as part of our overall core competency in HR, HCM, payroll and organizational success. We take a privacy "by design" approach that engages customers collaboratively.

Rely on our experience and partnerships to help you successfully manage today's personal data challenges. We are a certified SAP and SuccessFactors Business Process Outsourcing (BPO) partner as well as a leading SAP Human Capital Management and SuccessFactors consulting partner.

Taking It Personally…the Data Journey



Checklist & Takeaways

Zalaris is committed to helping all customers understand, meet and continuously adhere to new GDPR standards and guidelines. Whether you're in early or advanced stages of preparedness, we are the type of partner you can count on for quality support – including in conjunction with our advising partners and sub-processors.

Full compliance comes down to having the right practices and technical capabilities in place while also continuously reviewing, updating and refining corresponding measures. This checklist covers some key reminders but is not intended to be all-encompassing due to the complex and detailed nature of today's broader GDPR standards. We encourage you to engage Zalaris to more thoroughly cover all that needs to be done from both controller and processor standpoints.

- **Gap Assessment** - A holistic and thorough approach is employed to find and close any data privacy gaps that may exist or emerge relative to GDPR.
- **Governance Structure** - Data privacy policy is in place and closely adhered to with Data Protection Officer (DPO) appointed in independent oversight role.
- **Personal Data Inventory** - Personal data descriptions and flow charts are established and maintained for where data is held and processed, including between systems and countries.
- **Information Security** - Appropriate technical and organizational measures yield protections that are proportionate to risks internally and externally.
- **Operationalizing Data Privacy** - Strong policies and processes are fully in place, communicated, updated as needed, and enforced across the enterprise.
- **Training and Awareness** - Privacy training and awareness events are conducted as part of comprehensive overall GDPR compliance management program.
- **Third-party Engagement** - Effective controls and reporting validate IT and information security associated with external data processing, storage and disposal.
- **Monitoring and Reporting** - Integrated teams and tools support ongoing analysis and detection of possible or actual breaches as well as potential non-compliance issues.

Contact Us

Zalaris ASA

Postal address:
PO Box 1053 Hoff
NO-0218 Oslo, Norway

Visiting address:
Hovfaret 4b
NO-0275 Oslo
Telephone: +47 4000 3300
Telefax: +47 2202 6001

Website:
www.zalaris.com

eMail:
info@zalaris.com