



SecurityCompass

# How to Be GDPR Compliant with Article 25, Data Protection by Design and Default

SECURITY COMPASS

2018 Q2

---

## TABLE OF CONTENTS

<b>BACKGROUND .....</b>	<b>3</b>
<b>HOW TO INCORPORATE GDPR REQUIREMENTS INTO YOUR SOFTWARE .....</b>	<b>4</b>
<b>INTRODUCTION TO POLICY-TO-EXECUTION PLATFORMS.....</b>	<b>4</b>
<b>USING A POLICY-TO-EXECUTION PLATFORM TO PROVE DATA PROTECTION BY DESIGN AND DEFAULT.....</b>	<b>5</b>
Conceptual Model.....	5
Using SD Elements for General Controls .....	6
Content Subscription .....	7
Design Control & Define Rules.....	7
Start Project & Answer Questionnaire .....	9
Integrate with ALM .....	10
Learn and Implement Controls.....	10
Verify Controls & Integrate with Scanners .....	11
Review Reports .....	11
Using SD Elements for Contextual Controls .....	12
Set up appropriate permissions.....	12
Identify and eliminate redundant questions .....	12
Turn open-ended questions into closed multiple choice questions .....	13
Create controls on the right way to do something .....	13
Identify points of escalation and add notification triggers .....	14
Add context specific tasks directly into the project .....	15
<b>APPENDIX: RULES OF THUMB FOR CONTENT DEVELOPMENT .....</b>	<b>16</b>

## BACKGROUND

The European Union introduced the [General Data Protection Regulation](#) (GDPR) to improve the security of its residents. Going into effect on May 25, 2018, GDPR will impose steep penalties on organizations that fail to comply with its measures and has forced organizations around the world to increase their focus on privacy and security.

Several articles in GDPR affect software development, but one in particular will prove especially challenging for organizations falling under the new regulation: Article 25, “Data Protection by Design and Default.” This means the following:

**By Design:** “The controller shall...implement appropriate technical and organisational measures...which are designed to implement data-protection principles...in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”

**By Default:** “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed... Such measures shall ensure that by default personal data are not made accessible without the individual’s intervention....”

In other words, the controls outlined in GDPR must be built into the systems that process any personal data, such that full privacy is the default state of these systems.

Organizations will struggle to determine how to implement GDPR controls and incorporate these practices into rapid release cycle development methodologies such as Agile and DevOps. According to Gartner, over 75% of organizations have either adopted or will be adopting DevOps in an attempt to build software faster by the end of 2017. Accordingly, organizations are worried about how they will integrate security into DevOps. Left to the current mode of operations, organizations will be unable to meet the requirements of Secure by Design within DevOps.

Another major challenge for organizations will be proving that they have employed secure development practices and that these controls are working. As seen with the similar concept of [Privacy by Design](#) by Ontario’s Privacy Commissioner, Dr. Ann Cavoukian, proving adherence to Data Protection by Design and Default is not trivial.

Paper-based manual exercises such as questionnaires and software architecture reviews do not fit neatly into a fast-moving, automation-based DevOps model. Further, security tools such as Static Analysis Security Testing (SAST) demonstrate an absence of certain classes of security vulnerabilities, but are [not exhaustive](#) enough in coverage to prove that an organization has built in Data Protection by Design and Default.

## HOW TO INCORPORATE GDPR REQUIREMENTS INTO YOUR SOFTWARE

**Mandate Training:** One way to ensure that GDPR requirements are being taken into account when your software is developed is by educating your developers. Developers can be enrolled into a training program, such as “GDPR for Developers”, a 60-minute eLearning course targeted towards a technical audience which was developed by Security Compass. Trainees will learn about the critical elements of GDPR without having to dive too far into the minutiae of GDPR.

**Use a Policy-to-Execution Platform:** Fortunately, an emerging class of policy-to-execution platforms (such as SD Elements) can supplement training alone, and increases the capability for software development teams to achieve Data Protection by Design and Default, even in a fast-moving DevOps model. Let’s take a look at what they are and how they work.

## INTRODUCTION TO POLICY-TO-EXECUTION PLATFORMS



A policy-to-execution platform has four key capabilities:

- **Identify:** The platform will generate a specific list of relevant privacy & security controls or requirements for software based on a short questionnaire and boolean logic. These controls may include code samples, doing away with the need to maintain large, static secure programming guides.
- **Implement:** The platform should work with Application Lifecycle Management (ALM) tools like JIRA. To minimize impact on development teams, the controls become part of the application / product backlog just like functional user stories and other tickets. The platform tracks the status of controls being completed in the ALM solution and provide a single dashboard for the data protection team.

- **Validate:** The platform can integrate with automated Application Security Testing (AST) tools and validate which controls have been completed and which have not. Many privacy controls require human input to test, and the platform should provide instructions on how to manually test these controls.
- **Audit:** The platform should be able to provide reports on the current security and privacy state of an application, including its current compliance status with relevant sections of a standard or law like GDPR.

Critically, policy-to-execution platforms provide a means to add custom content above and beyond the content that comes “out of the box.” Thus, organizations can build their own questions, answers, and controls with rules. Customization allows organizations to tap into their own in-house expertise and scale the knowledge across their IT teams.

## USING A POLICY-TO-EXECUTION PLATFORM TO PROVE DATA PROTECTION BY DESIGN AND DEFAULT

### Conceptual Model

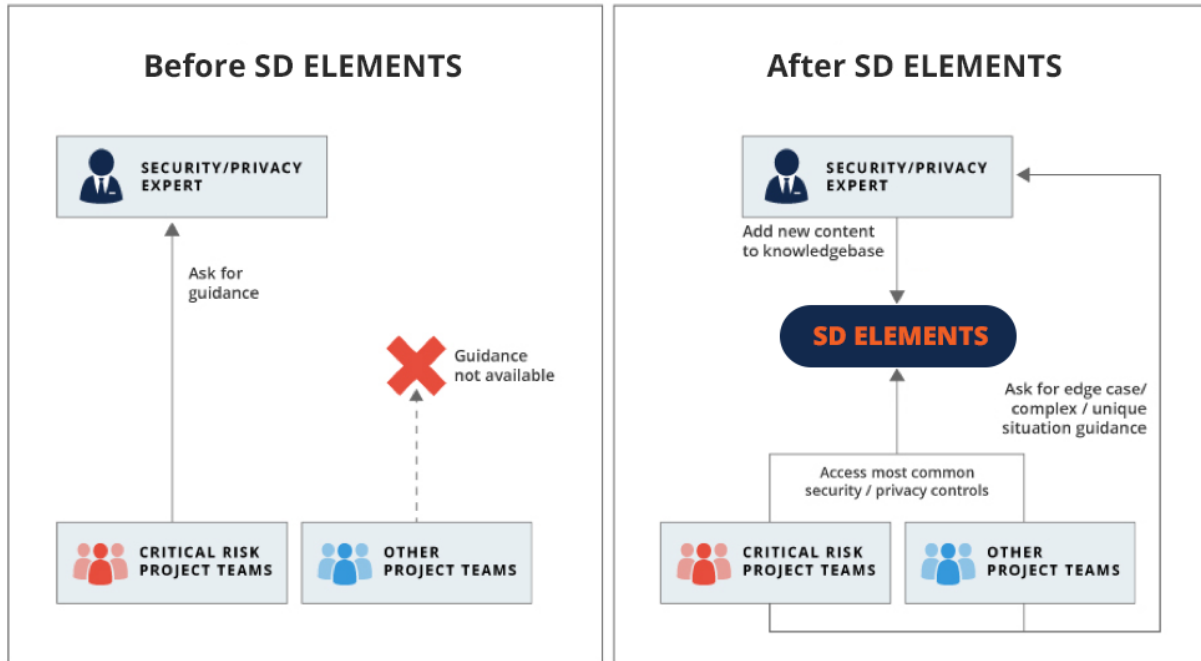
We can think of security and privacy design as having two kinds of outputs:

- **General:** Controls that apply to a wide variety of applications based on certain criteria. For example, “use a dialog box to ask for consent to store cookies” for any web application that uses tracking cookies in the EU.
- **Contextual:** Controls that are unique to a particular system and require human expertise to uncover. For example, the requirement to allow user avatar data to “be forgotten” in an online gaming system.

Many organizations [lack sufficient](#) in-house expertise to cover *all* of their project teams. They often use a risk-based approach where the most critical projects receive support from subject matter experts while other projects are left without support.

A policy-to-execution platform, such as SD Elements, provides a mechanism to automate the generation of general controls and reduce the overhead of creating contextual controls. Think of this platform as a way to scale your in-house or outsourced security and privacy expertise. Absent of a policy-to-execution platform, project teams need to work directly with expensive and difficult-to-find in-house experts or pour through clunky privacy and security standards documents to obtain controls. Apart from being too comprehensive to use effectively in short development cycles, reading documents does not provide the auditability necessary for proving compliance to a security or privacy standard or regulation.

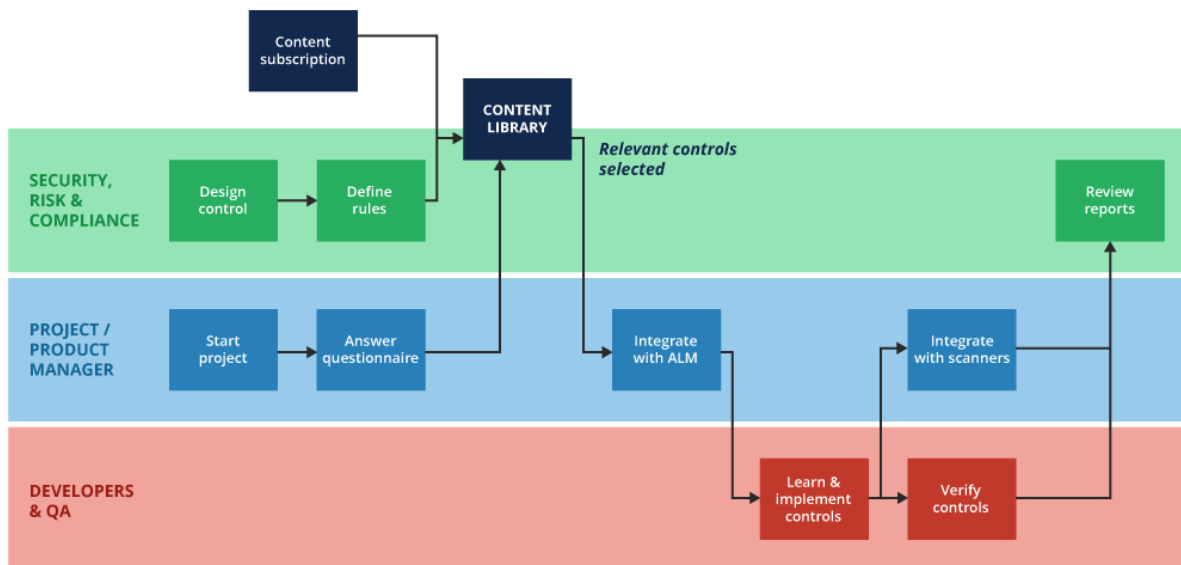
With SD Elements, experts add their knowledge of general controls into the library of content. Project teams access this content directly and then consult with experts for the areas not covered by the standard library. This allows a single expert to scale and meet the needs of more project teams.



Model of scaling security/privacy experts before and after using SD Elements.

## Using SD Elements for General Controls

Practitioners can make use of the following process to set up SD Elements to cover general controls.



General process flow diagram for a policy-to-execution platform.

## Content Subscription

A policy-to-execution platform vendor, such as Security Compass, has a team of researchers that produce content for certain controls, such as secure coding and server hardening. That content grows and is revised on a regular basis. The controls library for the organization encompasses both the subscription content as well as custom organizational content.

T180	Provide privacy preferences to the browser via P3P
T187	Test if the app prevents sensitive data leaks through the auto-snapshot feature of iOS
T188	Avoid storing cached confidential data in flash memory
T194	Obtain user consent for tracking cookies

*Examples of out-of-the-box SD Elements privacy controls.*

## Design Control & Define Rules

On top of the out-of-the-box content, security, risk and privacy/compliance stakeholders will want to append additional content specific to their organization and context. For example, for GDPR they may wish to include requirements based on recent rulings about features related to data crossing international borders. They may also need to expand the questionnaire to include additional questions, while keeping the length of the questionnaire manageable (see [Four Rules of Thumb for Developing Content](#)).

SD Elements makes it easy to define new content that is configured by rules using a guided user interface:

## Add New Task

Title ?

Priority ?

*Adding a new task and assigning a priority in SD Elements.*

### Applicable to a Project when

the following rules are met:

Type of Application - Web application AND  
Programming Language - JavaScript

[Edit](#) | [Cancel](#)

[+ Add Another Rule](#)

*Setting up the applicability rules for a new task in SD Elements.*

In this process, you can also (and are encouraged to) cross-check internal policies, procedures, guidelines, and baselines to see if there are any privacy-related controls that you should add to the content library.

Every control should also have a corresponding validation process. In a policy-to-execution platform, this could be a “Testing” phase task that is linked to the control via an underlying problem. In more advanced use cases, controls may be automatically verified with a separate tool, such as a configuration review tool, that integrates with the policy-to-execution platform via API.



## Add New Task

Title ?

Verify that third party libraries have privacy policies which require data minimization

Priority ?

*Adding a corresponding testing phase task in SD Elements.*

### Start Project & Answer Questionnaire




With the content ready, you can begin to model applications into the SD Elements. In the pilot phase, security or privacy experts often perform this step. In a full deployment, project managers, project owners or architects from the project teams often take ownership of this step, effectively creating a self-service model.

The process of modelling an application involves creating a new project in SD Elements and answering the questionnaire.

Organization	<b>Handles Personally Identifiable Information</b>	<b>Privacy Regulations</b>
Financial Systems	<input checked="" type="checkbox"/> Yes ?	<input checked="" type="checkbox"/> GAPP ?
Health Care Systems		<input type="checkbox"/> PIPEDA ?
Industrial Control Systems		<input type="checkbox"/> ECPA ?
Privacy		<input type="checkbox"/> GDPR ?
Compliance Scope: Other		<b>Handles the Following Types of Sensitive Personal Data:</b>
		<input type="checkbox"/> Religious or ethnic origin
		<input type="checkbox"/> Political opinion
		<input type="checkbox"/> Religious or philosophical beliefs

*Examples of out-of-the-box SD Elements privacy questions.*

Once completed, SD Elements will produce a prioritized list of controls.

 DONE	<b>10</b>	<b>CT1: Disable use of the Struts REST plugin</b>	Due to detected attacks related to the recent Apache Struts vulnerability, development teams should disable...	<a href="#">Add Note</a>   <a href="#">Assign User</a>   <a href="#">Verification</a>
 TODO	<b>10</b>	<b>T327: Review security of Node.js modules before installation</b>	The Node Packaged Modules (NPM) tool offers a simple and powerful means for installing Node.js package repository and there is no guarantee that the modules are not malicious or insecure.	<a href="#">Add Note</a>   <a href="#">Assign User</a>   <a href="#">Related Tasks</a>   <a href="#">Verification</a>
 TODO	<b>9</b>	<b>T35: Fine-Tune HTTP Server Settings</b>	Set limits on incoming HTTP messages, and configure the HTTP server to reduce risk.	<a href="#">Add Note</a>   <a href="#">Assign User</a>   <a href="#">Related Tasks</a>   <a href="#">Verification</a>

*Example list of tasks (ie. controls) for a project in SD Elements.*

You can further filter the list to only focus on data privacy controls, or you can more holistically review all controls including security.

For existing systems, a technical lead should go through the resulting list of controls and mark any already-implemented controls as “Done.”

### **Integrate with ALM**

After defining the correct set of operational controls, you can add the incomplete controls to the development queue of work. In an agile or DevOps workflow, this means adding it to the product backlog. In a more traditional / waterfall project, this means introducing the controls as requirements into the current or next release.

With SD Elements, you can integrate directly with an Application Lifecycle Management (ALM) tool such as Atlassian’s JIRA and many more.

### **Learn and Implement Controls**

Once pushed into the backlog or requirements list, developers can complete controls one at a time alongside normal feature work. In cases where they cannot complete a control, the developers can leave a comment either in their ALM or within SD Elements directly explaining why.

## Verify Controls & Integrate with Scanners

The final step in the process is to verify whether controls are completed accurately. For a certain subset of controls, this may be accomplished by integrating results from a scanner. For others, this will require manual testing steps completed by a developer, tester or security / privacy SME. Alternatively, development teams may be able to set up automated testing scripts to verify controls.

## Review Reports

To provide audit evidence for the future, the project manager and security, risk and compliance stakeholders can produce reports to show the status of a project.



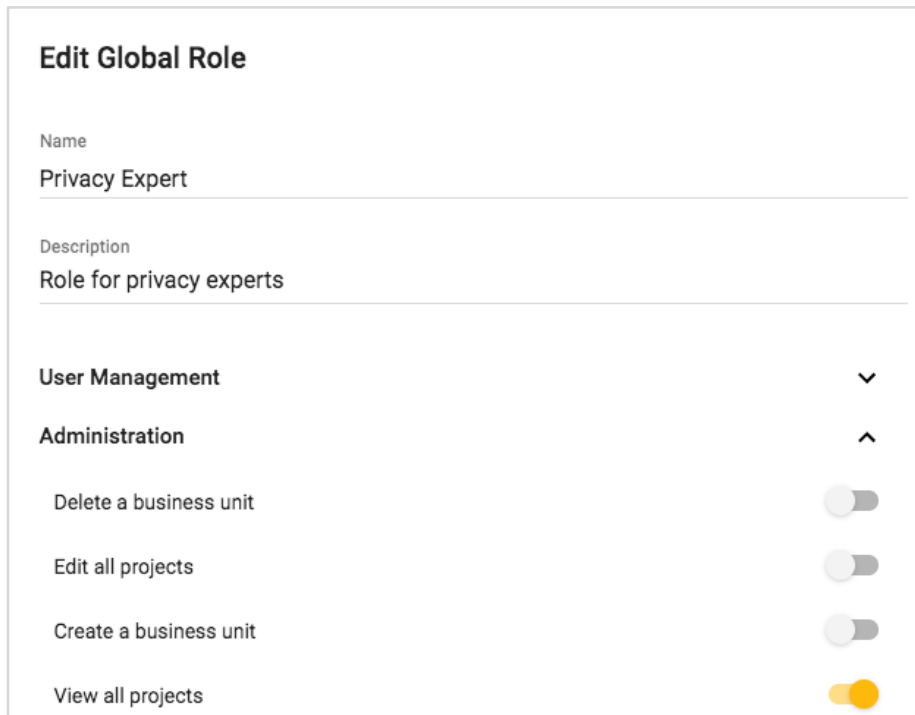
Front page of GDPR compliance report from SD Elements.

## Using SD Elements for Contextual Controls

SD Elements also allows users to incorporate contextual controls, a process that differs slightly from general controls. Here we will review how to translate the key parts of a Privacy Impact Assessment template into such a platform.

### Set up appropriate permissions

To facilitate activities, central privacy or security experts should have access to all projects.



**Edit Global Role**

Name  
Privacy Expert

Description  
Role for privacy experts

**User Management** ▼

**Administration** ▲

Delete a business unit

Edit all projects

Create a business unit

View all projects

*User role management example from SD Elements.*

### Identify and eliminate redundant questions

A typical PIA asks a series of questions about the project or system in-scope, many of which are already in SD Elements out-of-the-box. For example:

- Application name
- Business unit (if applicable)
- Architecture type (e.g. web application)

Keep the Don't Repeat Yourself (DRY) principle in mind.

## Turn open-ended questions into closed multiple choice questions

Many of the remaining questions of a typical PIA are open-ended in nature. For example, some PIA templates ask questions like, “List each data type being collected.” Broad questions like these are onerous to answer and slow down the development process considerably. Instead, use a pre-populated list and a single “Other” option if you want people to specify a different option.

Personally Identifiable Information Types
<input type="checkbox"/> Names
<input type="checkbox"/> Address
<input type="checkbox"/> Email address
<input type="checkbox"/> Phone number
<input type="checkbox"/> Credit card number
<input type="checkbox"/> Social insurance / security number
<input type="checkbox"/> Social media identifiers
<input type="checkbox"/> Protected health information
<input type="checkbox"/> Other personally identifiable information

You can then create a control that asks users to specify what the text means, which only shows up in a project when they select the “Other” option:

### Add New Task

Title <sup>?</sup>  
Describe other PII in the notes field

Priority <sup>?</sup>  
10 - High Priority

Phase <sup>?</sup>  
 Requirements  Architecture & Design  Development  Deployment  Testing

**Applicable to a Project when**  
the following rules are met:

Personally Identifiable Information Types -  
Other personally identifiable information  
[Edit](#) | [Cancel](#)

[+ Add Another Rule](#)

## Create controls on the right way to do something

Instead of asking a question like “Describe your privacy policy,” create controls that specify the minimum standards of a privacy policy for your organization.

Use the flexible rules-based engine to create derivative controls for unique circumstances. For example, the privacy policy of a website based in Europe may differ from one in the United States.

The control should also have a “Testing” phase control that testing teams can use to validate that a control has been met.

### Identify points of escalation and add notification triggers

There may be certain circumstances where manual intervention in the process is warranted. For example, if the system stores processes or transmits sensitive information such as health data. In this case, you can create a control similar to the above and add an email trigger to a specific user, such as a privacy expert, for when that control shows up. This also serves as a useful way to determine which projects your security and privacy experts should perform a deeper dive into.

*Setting up email alerts for a specific task.*

### **Add context specific tasks directly into the project**

Subject matter experts who review a project in SD Elements may identify specific, contextual controls for that project that are not already in the system.

They can do this by using the “Add task” button from within the project.



With SD Elements, organizations can meet GDPR compliance without sacrificing efficiency, and can do so in an auditable framework that proves compliance and provides accountability.

[Visit our website](#) to learn more about [SD Elements](#), an award-winning policy-to-execution platform.

[Visit our website](#) to find out how you can enroll your developers in GDPR training and see what other software security courses we offer.

## APPENDIX: RULES OF THUMB FOR CONTENT DEVELOPMENT

- **Minimize impact:** Do not impose a control unless it is necessary. For example, do not ask a development team to implement privacy controls if they are not collecting, storing or processing personally identifiable information.
- **Don't repeat yourself:** Developers should not be answering the same questions multiple times for different stakeholders. Ask them to answer once and use the same data in multiple places. It is also important to contain the size of the initial questionnaire; if it takes longer than 15 minutes to complete the questionnaire, you may start to get feedback.
- **Use priorities:** Providing a new project with 100 new controls is likely to be met with extensive pushback. Use prioritization so that development teams can implement the controls and prioritize them alongside other features.
- **Controls over open ended questions:** Provide controls about what somebody should do, rather than asking an open-ended question that requires an expert to interpret. Allow developers to specify why they can't implement a control and the reason why. Use "Describe" questions sparingly.
- **Testability:** Controls should be easily testable. For example, "Validate a consent form for cookies appears upon session initiation."
- **Make changes easy:** Do not make people answer an entire assessment for each change. Instead, determine which questions and controls are likely to require reaffirmation and ask them instead. Strive to make the process last minutes instead of hours.



## ABOUT SECURITY COMPASS

Security Compass is a leader in helping customers pro-actively manage cybersecurity risk, without slowing down business. Offering SD Elements, Just-in-Time Training, and Enterprise Delivery Services, as well as Verification Services, we help your organization efficiently deliver technology that's secure by design. At the core of our solution is our policy-to-execution software platform, SD Elements, which translates policies into actionable tasks for technical teams. Security Compass services some of the world's largest enterprises, as well as 4 of the largest tech companies in the world. We're headquartered in Toronto with global offices in the United States and India. Follow Security Compass on Twitter @securitycompass or visit <https://www.securitycompass.com/>

## PARTNERS & AWARDS



# Security Compass

Making Software Secure

[www.securitycompass.com](http://www.securitycompass.com)

[info@securitycompass.com](mailto:info@securitycompass.com)

+1 (800) 777-2211