EUgrc GDPR Compliance Suite

Helping you prepare

Getting ready for the EU General Data Protection Regulation will be a challenge for most organisations dealing with data about European natural and legal persons.

With little time left until this regulation takes effect, many companies are just now starting out on their compliance journey – and finding that qualified help is not readily available, or, if it is, costs a small fortune...

EUgrc's goal is to make GDPR compliance less confusing, less painful and less expensive (both in terms of how much your compliance programme costs, and in terms of not having to pay penalties which can be as large as €20 million or 4% of your global turnover).

> "Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use."[1]
>
> *- ELIZABETH DENHAM, UK INFORMATION COMMISSIONER*

Available on ORACLE Cloud Marketplace

[1] Quotes are taken from a speech which Elizabeth Denham delivered at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017. The inclusion of these quotes are purely informational in nature and in no way are meant to state or imply any endorsement of EUgrc's products or services by Elizabeth Denham or the UK ICO. The full text of the aforementioned speech may be accessed here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

How to prepare

Once both you and your organisation's management are aware of what the EU General Data Protection Regulation is all about (and, yes, there's tonnes of good information already on the web about it), getting ready for the GDPR can be summarised in a few key steps:

1. **Understand and control** who does what with your data. Those individuals are called "Actors" and they can have roles like data controller, data processor, data provider and data recipient. Make a list, check it twice, understand who they are, what data they work with (and why), where they are located, etc.
2. **Understand what tools are used to work with your data.** Data doesn't exist in a vacuum, it's stored someplace, transferred by certain tools, worked with using other tools, safely deleted/destroyed using still other tools. Each of those tools has certain risks and threats associated with it – whether it be someone stealing paper documents with personal information, or a sophisticated software hack, or, simply a fire that destroys some data. You need to know what you use and how you use it, so you can plan appropriate safeguards to keep that all-important data private.
3. **Understand your data.** What personal data do you collect and hold? Who are the data subjects? Are any of them children (in your jurisdiction, or in their home country – the definition of "child" varies in the EU…) What's your business purpose for doing so? Is any of that personal data super sensitive? Have you put in place all appropriate safeguards? And, is collected and using that data permitted under the General Data Protection Regulation.
4. **Perform your Privacy Impact Assessments / Data Protection Impact Assessments.** Understand your risks. Make informed choices which risks need to be treated and treat them, and, which risks you are prepared to accept.
5. **Dust off the good old Deming Cycle – plan, do, check and act.** Make a plan, implement it, evaluate your results. Has the plan brought your level of risk down to acceptable levels? What else can you do to improve the security and privacy of the data you control or process?
6. **Get your paperwork in order.** Make sure you have documented all necessary procedures, starting from the basics like an information security policy and consent forms, all the way to contractual clauses for your contractors and suppliers, templates for notifying people about data breaches and how to deal with access requests by data subjects.

Getting all of this done in less than 5 months can be a big challenge. Finding available and qualified consultants to help you – even harder. We know. We went through this process ourselves and have helped organisations across Europe and North America do it, too.

That's why we decided to automate and simplify the process. The EUgrc GDPR Compliance Suite gives you your own personal GDPR consultant that's available to you 24 hours a day at the click of a mouse.

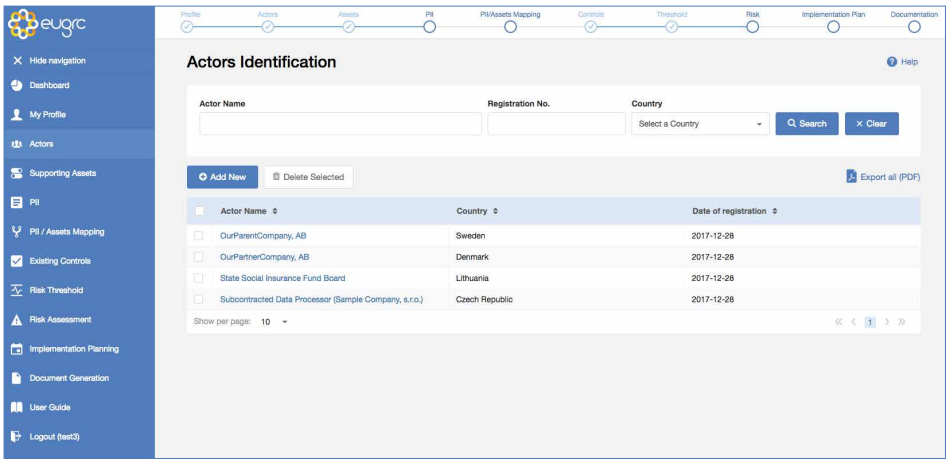
> "When it comes to data protection, small businesses tend to be less well prepared. They have less to invest in getting it right. They don't have compliance teams or data protection officers. But small organisations often process a lot of personal data, and the reputation and liability risks are just as real."
>
> *- ELIZABETH DENHAM, UK INFORMATION COMMISSIONER*

Making Compliance Happen with the EUgrc GDPR Compliance Suite

Understanding who does what

As a data controller, you have a responsibility for how the personal data you control is processed on your behalf, regardless of whether you do this in-house, or whether you have a contractor do it for you. Using GDPR-related terminology, someone who does something with personal data is considered an Actor. Actors can be data controllers, data processors, data providers or data recipients.

EUgrc's GDPR Compliance Suite lets you quickly and easily inventory and record all actors involved with the personal data you control. With just a few keystrokes, you can record not only basic information about the actor, but also clearly match the actor with the specific personally identifiable information sets with which they work.

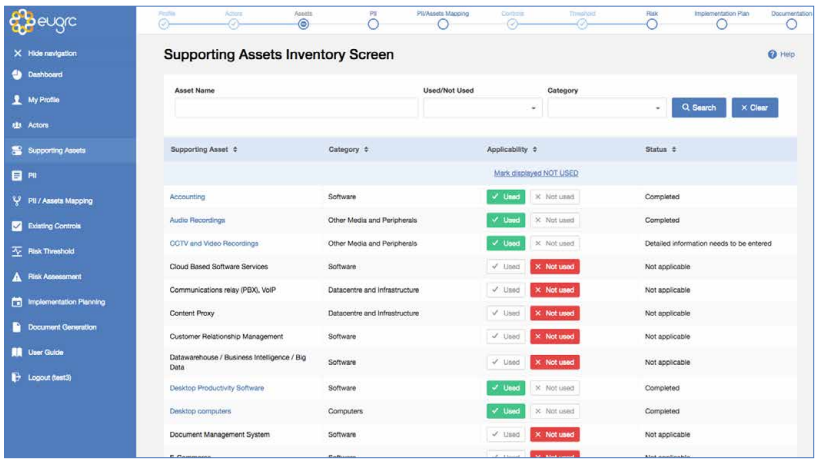


Actors entered into the Suite can be reviewed, edited, assigned to new PII data sets, removed and exported for your convenience in PDF format.

Understanding the tools used with your data

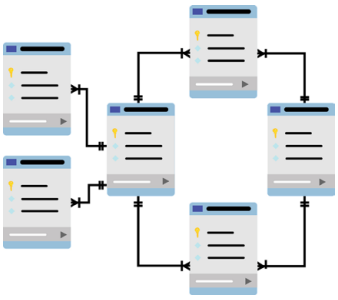
It's important to know what hardware, software, paper or people are involved with a particular personally identifiable information data set, because each of these things has specific vulnerabilities and risks associated with it. We call these items Supporting Assets, since they support your information collection, processing, transfer and deletion activities.

The EUgrc GDPR Compliance Suite comes preloaded with a wide range of Supporting Assets. The user simply tells the system if they use or don't use a particular asset. If an asset is marked as Used, the system pre-loads a quick questionnaire about the types of controls you should apply to keep the data accessed with that asset safe.

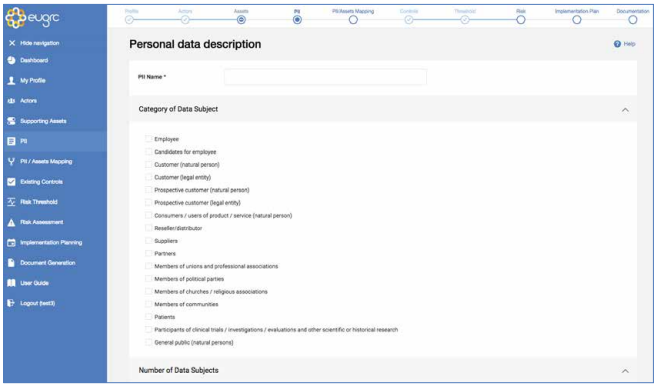


This saves you valuable time. You don't have to research the appropriate controls for each asset type. You just need to quickly review a list of guided questions and answer them Yes or No (or, sometimes, Not Applicable).

Understanding your data



GDPR is all about data. To keep that data safe and private, you must know what you're collecting and processing, the purposes for doing so, and how those two things relate to legal requirements. **EUgrc's GDPR Compliance Suite** lets you easily catalogue your personally identifiable data sets. And, not just describing the fields included in the data set, but reviewing the data set's compliance with legal requirements at the same time.



- Do you have a legitimate business purpose for collecting and processing that data? What is your legal justification for doing so in terms of the GDPR?
- Who are the data subjects? Is there any highly sensitive information in the data set?
- Where do you get the data? Who is the data controller, data processor, data provider and data recipient?
- Have you assigned a Data Privacy Officer (DPO)? Who is it? What about the business owner?
- How long do you store that data? Why do you store it for that retention period?
- What controls do you have in place to keep the data secure and private?
- And more…

Answering these questions on paper or in a spreadsheet is a challenge. Especially since without a consultant, it's not always easy to know which questions you should ask yourself.

Our solution takes care of that headache and guides you through a single screen that allows entry of all needed information about a personally identifiable data set.

Perform Data Protection / Privacy Impact Assessments and Risk Assessments

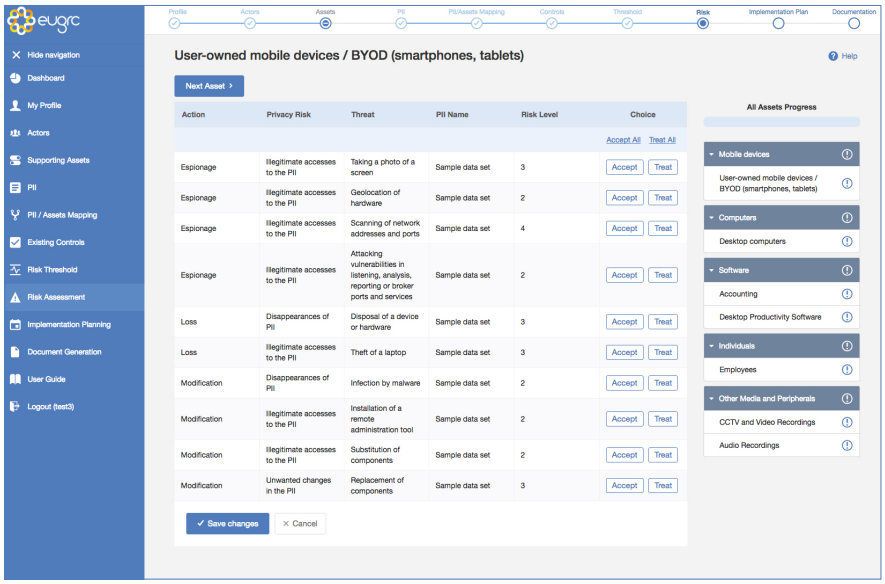
Here's where it gets tricky. In order to do this step on your own, you need to do a lot of research. Get to know the legislation, understand the relevant ISO/IEC standards, get a lot of knowledge about the privacy risks, threats and vulnerabilities associated with different types of supporting assets, keep track of new threats and vulnerabilities as they arise, know what controls affect which risks. Then – evaluate it all, put it into an algorithm, crunch your data and get an answer.

Sounds complicated, right? And, it is… But, EUgrc's GDPR Compliance Suite has all of this built in. By answering some simple questions about your actors, data sets, supporting assets and your existing controls, the system **automatically and painlessly** conducts the PIA / DPIA for you.

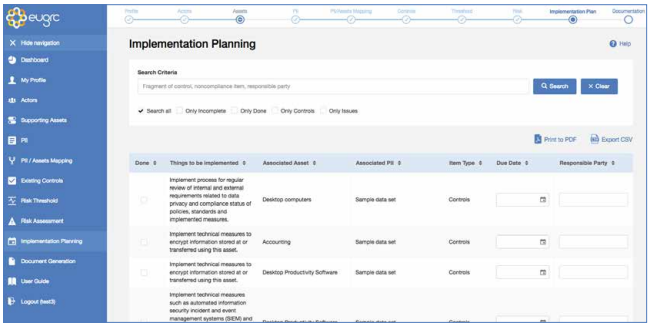
You choose the level of risk that's acceptable to you. You choose whether to review just the high risks and accept those below your acceptable risk threshold, or to review everything.

> "The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."
>
> *- ELIZABETH DENHAM, UK INFORMATION COMMISSIONER*

Once you've made your choice of a risk threshold, the system **guides you** step-by-step through your risks, allowing you to make informed choices about which risks you want to accept, and those that must be treated.



Planning and making needed changes



Knowing about the risks to the personally identifiable information you control or process is one thing. Doing something about it is another. There's no point in doing a Data Protection Impact Assessment / Privacy Impact Assessment if you don't make needed changes.

To make the changes happen, you need good advice about what needs to be done to bring risk down to acceptable levels.

EUgrc's GDPR Compliance Suite takes the guesswork out of the equation. Our system is preloaded with the experience of hundreds of information security and data privacy consulting projects and will generate a detailed implementation plan for you.

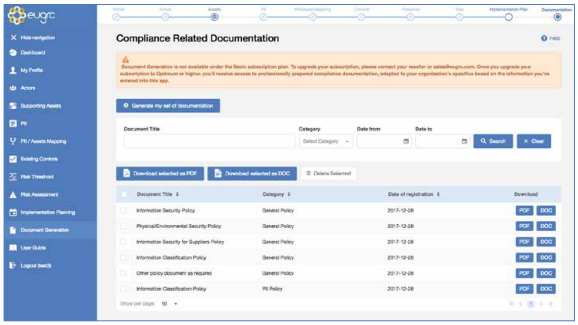
Once the plan is generated, you can assign responsible persons in your organisation, assign due dates, and track progress. When a task is completed, mark it as done and watch as your risks are automatically re-calculated, showing your progress in bringing those risks down to an acceptable level.

This plan can be used in the system, or, if it's more convenient for you, exported and then imported into your organisation's usual task management system.

Getting the paperwork right

If you use a search engine and look up "GDPR Compliance Kit" on the internet, you'll find a tonne of offers for "templates" that you can download. These sites are right in the sense that you need to get your paperwork right to comply with the EU General Data Protection Regulation.

But, they're wrong in the sense that one set of templates can be applied to hundreds of different organisations.



The EUgrc GDPR Compliance Suite has a compliance document generation function[2] that gives you needed policies, standards, consent forms, clauses to add to contracts with your suppliers or employees, and more. Generated documents are adapted to your organisation's specifics based on the information you entered in the previous steps.

The documents can be downloaded either in PDF or a format editable in any popular desktop productivity suite. If you change some of your data, you can re-generate your documents, saving you time in editing them on your own.

[2] Note: this functionality is not available at the Basic subscription level, you must have an Optimal or Premium subscription to use this function.

About EUgrc

EUgrc is a consortium owned and operated by VORAS Consulting Ltd. and the iTree Group family of companies. VORAS Consulting works with organisations worldwide in ensuring information security, compliance, data privacy and prevention of Cyber Attacks. Over 100 successful projects delivered in the EU, United Kingdom and the United States of America attest to our experience.

The VORAS team's experience and knowledge is attested to by numerous CISSP, ISSMP, CISM, CISA, CGEIT, CRISC, PMP, OSCP, CEH and LPT certifications. Our information security management system is certified by Bureau Veritas as compliant with ISO/IEC 27001 and our IT Service Management System is certified as compliant with ISO/IEC 20000, as well.

The iTree Group family of companies deliver enterprise technology solutions for the insurance, financial services, utilities, energy, oil & gas, and, the public sector. Solutions include Oracle® ERP and core P&C insurance system implementation, custom development on Oracle DB and Java, system support and maintenance, and, productivity engineering.

ORACLE Platinum Partner

iTree is a Platinum Worldwide Oracle® partner with 16 Oracle-awarded specialisations and we serve our customers through a wide network of offices.

See **https://eugrc.com** for more information, pricing and ordering.