GDPR COMPLIANCE: HOW AUTOMATION CAN HELP

September 2018

DISCLAIMER

This white paper is a commentary on the GDPR, as Chef interprets it, as of the date of publication. We like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled. As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

CHEF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other Internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Chef product. You may copy and use this white paper for your internal, reference purposes only.

The requirement to show compliance to GDPR is here. While organizations are rightfully concerned with compliance to avoid heavy fines, the GDPR mandate offers an opportunity to introduce an automated approach to managing compliance with long lasting benefits. GDPR enforces the concept of "privacy by design," meaning security and regulatory compliance can no longer be treated as bolt-ons or afterthoughts. By applying continuous automation to GDPR requirements, organizations can build compliance and security principles into the development cycle, reducing risk while enabling speed to market and competitive advantage. GDPR compliance can be approached as a journey to continuous automation - detect, correct,
and automate.

INTRODUCTION TO GDPR

In April 2016 a new set of data protection principles were adopted by the EU Parliament. These principles replace previous disparate pieces of policy relating to personal data and are designed to bring EU policy up to date with the digital age. This new General Data Protection Regulation (GDPR) contains requirements to help organizations meet their data protection responsibilities in the EU. GDPR became a compulsory requirement in May 2018.

WHO IS SUBJECT TO GDPR?

The intention of GDPR is to create a holistic and harmonised policy that covers all EU member states, including the UK. It applies more broadly than might be apparent at first glance. Your business must comply with GDPR if you meet the following criteria:

- **You offer goods and services to individuals in the EU; or**
- **You collect and analyze data tied to individuals in the EU**

It is important to note that GDPR does not only apply to business in the EU, but to businesses globally that trade goods and services with EU citizens or business entities. The GDPR applies to you if you are established in the EU, if you offer goods or services in the EU, or if you monitor the behavior of individuals in the EU.

WHAT ARE THE IMPLICATIONS OF GDPR?

GDPR comes with a number of key requirements that impact various areas of a business.

1. **BREACH NOTIFICATION** - any data breaches must be reported to the supervisory authority within 72 hours of being identified, unless an exception applies.

2. **RIGHT TO ACCESS** - data subjects (EU citizens) can access data being stored on them for free.

3. **RIGHT TO BE FORGOTTEN** - data subjects can submit a request to have their data deleted free of charge.

4. **DATA PORTABILITY** - subjects should be able to retrieve their data in an easy to understand way.

5. **PRIVACY BY DESIGN** - data protection should start at the design stage of systems.

6. **DATA PROTECTION OFFICERS** - these are now internalised and based on record keeping.

Should a company fail to meet these requirements and fail to demonstrate their GDPR compliance they could be subject to fines up to the greater of:

- **€20 million** OR

- **4% of annual global turnover (total sales volume, net of all discounts and sales taxes)**.

ACHIEVING AND SUSTAINING GDPR COMPLIANCE

The stringent GDPR requirements compel organizations to act decisively. But in today's business environment, where apps are the customer interface and competitive success demands an ability to deliver software quickly, compliance efforts risk slowing business growth. Indeed, Gartner reports that 81% of IT operations professionals say they believe InfoSec policies slow them down. InfoSec professionals agree, with 77% sharing the same view[1]. How can an organisation move quickly without compromising the levels of control needed to be in place to meet the GDPR requirements?

The answer lies in extending DevOps practices to achieve continuous automation, whereby teams move faster while managing down risk. Today three-fourths of organisations are in some phase of DevOps adoption[2], applying agile, lean, and DevOps (ALDO) principles to create streamlined processes with the flexibility to adapt quickly to change. By defining the auditing toolset in code, organisations can automate compliance the same way they are automating infrastructure and other aspects of their operation. With GDPR looming, defining and executing an achievable roadmap is even more crucial.

GDPR AUTOMATION ROADMAP

As with any new project, it is vital that there is a clear and widely communicated roadmap. The same is true for GDPR compliance automation.

The most successful organisations, who undertake a digital transformation program, follow recognised patterns and behaviours to achieve their goals. This model covers the following steps:

1. **DETECT** - automate the detection and collection of GDPR compliance failures
2. **CORRECT** - apply remediation consistently and at scale
3. **AUTOMATE** - build the detect and correct workflow into existing practices.

[1] Gartner—DevSecOps: How to Seamlessly Integrate Security Into DevOps 2016

[2] Rightscale—2016 State of the Cloud report

DETECT - GDPR Compliance as Code

A new breed of tools for managing infrastructure, systems and application deployment in code are well established in the IT industry. Chef is leading the way and redefining Compliance by treating it as code.

A code driven approach to GDPR compliance builds on existing methods for collaboration already used by DevOps teams. Chef software can employ a control-based approach to defined security regulations and turn these into small, modular, executable blocks, which, combined, can illustrate and implement any security policy.

MEET INSPEC

To redefine compliance, a new way to describe it is required. InSpec provides exactly that. InSpec is human-readable, versionable, highly customisable and treated like any other code base. Instead of relying on static documents for compliance verification, InfoSec professionals describe GDPR controls in the InSpec language.

6.2.1 Set SSH Protocol to 2 (Scored)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^Protocol" /etc/ssh/sshd_config
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

```
control 'ssh-1234' do
  impact 1.0
  title 'Server: Set protocol version to SSHv2'
  desc "
    Set the SSH protocol version to 2. Don't use legacy
    insecure SSHv1 connections anymore...
  "

  describe sshd_config do
    its('Protocol') { should eq('2') }
  end
end
```

By grouping these controls, InfoSec professionals can create a corporate profile that can be shared across the business and executed on any system and environment.

InSpec code can then be executed in an audit scan either as a triggered task or as part of a continuous scanning policy.

GDPR AS INSPEC -

1 - SECURING WORKSTATIONS

Scenario: *a consumer research company has employees that regularly handle EU citizen data on their workstations. The software company wants to audit their workstations and prove that they are locked down with appropriate password complexity.*

Example InSpec Control:
Check that the Windows workstation local security policy is configured correctly.
https://github.com/chef-cft/gdpr_examples/blob/master/controls/password_complexity.rb

The local security policy is checked to make sure that suitable password complexity is enforced.

2 - DATA STORAGE

Scenario: *a travel company stores large amounts of data about their EU customers in clustered databases. The travel company needs to make sure that all of their databases are configured and secured correctly.*

Example InSpec Control:
Assess the database configuration file to make sure it has all the settings needed.
https://github.com/chef-cft/gdpr_examples/blob/master/controls/database_security.rb

3 - TIGHTENING ACCESS

Scenario: *a large UK IT outsourcer is running back office IT environments for a number of financial services organisations. Varying amounts of personal EU citizen data passes through these systems. The UK IT outsourcer needs to scan local firewalls across ALL of their Windows Server systems to identify any misconfigurations.*

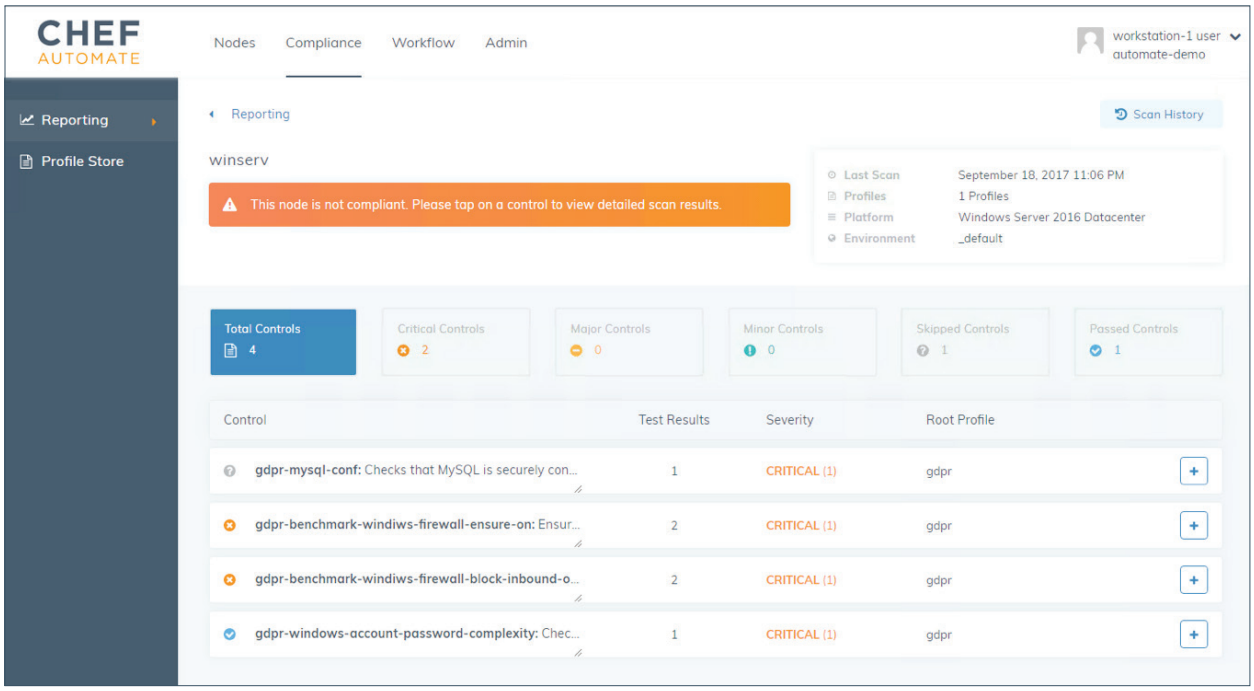
Example InSpec Control:
Check that the firewall is running and properly configurated.
https://github.com/chef-cft/gdpr_examples/blob/master/controls/access_control.rb

REPORTING - DATA DRIVEN DECISION MAKING

Having executed the InSpec tests, the compliance scan results should then be actionable.

All audit scans carried out using InSpec across each system within an organisation are centrally aggregated and reported on.

The Chef Automate platform provides a granular reporting capability with detailed views of system state. This informs IT teams and helps them direct their efforts to correct any issues that may impact your business' GDPR compliance.



Chef Automate provides historical data sets allowing compliance trends to be tracked, identifying potential issues quickly so corrective measures can reduce potential impact.

CORRECT - automated remediation

Identifying GDPR compliance issues is important, but the ability to correct them at scale, consistently, and predictably is a unique benefit of an automated approach.

Chef, the configuration management tool, is widely used and leads the way on platform support and enterprise tooling. It is used to apply consistent configuration at scale across IT systems, networking devices and infrastructure.

InSpec can be used in conjunction with Chef client or in isolation for environments with regulatory requirements that demand a separation of duties between compliance auditing and system management.

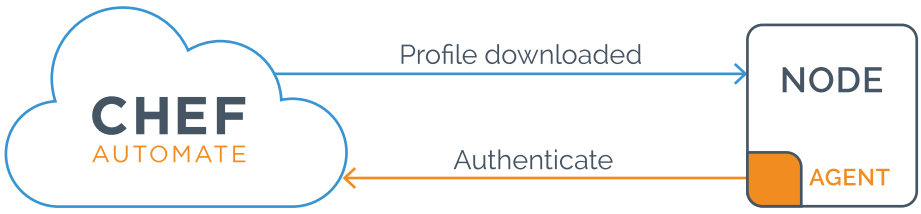
From an auditor's perspective, a business must be able to demonstrate how an identified risk is treated or accepted, and the criteria used to make that decision. When a risk is treated, the path from detection to correction should be simply and repeatedly demonstrable.

This is where the tight integration between InSpec (detect) and Chef (correct) greatly reduces the burden on IT teams when it comes to conforming with their GDPR requirements and demonstrating that their systems are built with '*privacy by design*'.

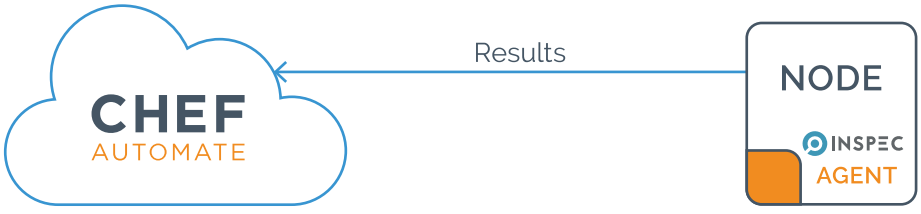
DETECT AND CORRECT - A CONSISTENT MECHANISM

Using the Chef language and the Chef Automate platform allows a continuous workflow, including remediation, to be established.

1. A target machine, or node, is configured with the Chef agent. The agent authenticates with the Chef Automate platform to retrieve a Compliance profile and execute an audit scan.



2. Scan results are reported to Chef Automate allowing the operator to remediate identified GDPR issues. Chef configuration code is written.



3. On the next agent run the configuration code is retrieved, and applied locally, then an audit scan executes as part of the same run. The improved results are reported back to Chef Automate allowing further remediation to be identified.

AUTOMATE - Continuously Delivering Compliance

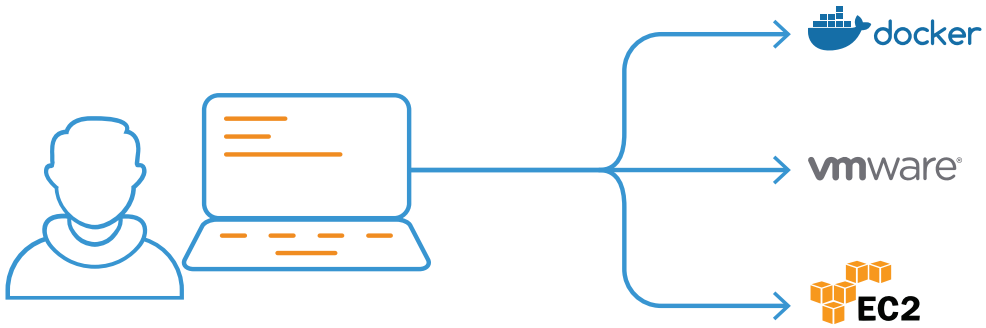
For GDPR compliance efforts to be effective they need to align with existing business processes. Many IT organisations have existing processes in place, automated or manual, for creating and deploying new IT environments. The following examples demonstrate how GDPR Compliance with InSpec and Chef Automate can become a seamless part of day to day operations.

THE DEVELOPMENT WORKFLOW

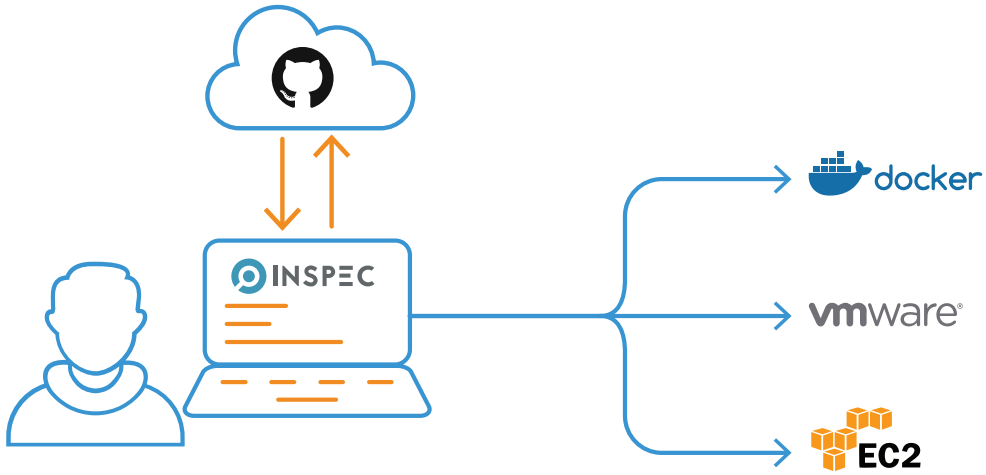
Many organisations follow the development to testing / QA to staging to production workflow. A common challenge is the interface between these different teams and environments. How can it be ensured that a change made by a developer doesn't impact a system further down the lifecycle?

The solution is to make GDPR compliance scanning an integrated part of the development team's behaviour. The InSpec command line tool can pull a profile from the existing version control system and run it against a developer's test machine, regardless of whether that machine is local, a container or a cloud virtual machine.

Step 1 - the developer is writing their app code and testing it in their development environment. Once they're happy with how it works, they need to push their changes into version control.



Step 2 - before pushing those changes,they use the InSpec CLI to execute a compliance scan. The CLI retrieves the business GDPR profile from version control and runs it against their dev environment. If all is well they can commit their code. If not, a potential vulnerability is identified before getting anywhere near production–like systems.



INFRASTRUCTURE ORCHESTRATION

An important part of ALDO is to treat all layers of an application stack in code. The same is true for infrastructure- whether autoscaling in a cloud environment, or automating the deployment of complex on-premise vmWare deployments, there are a number of options when it comes to tooling.

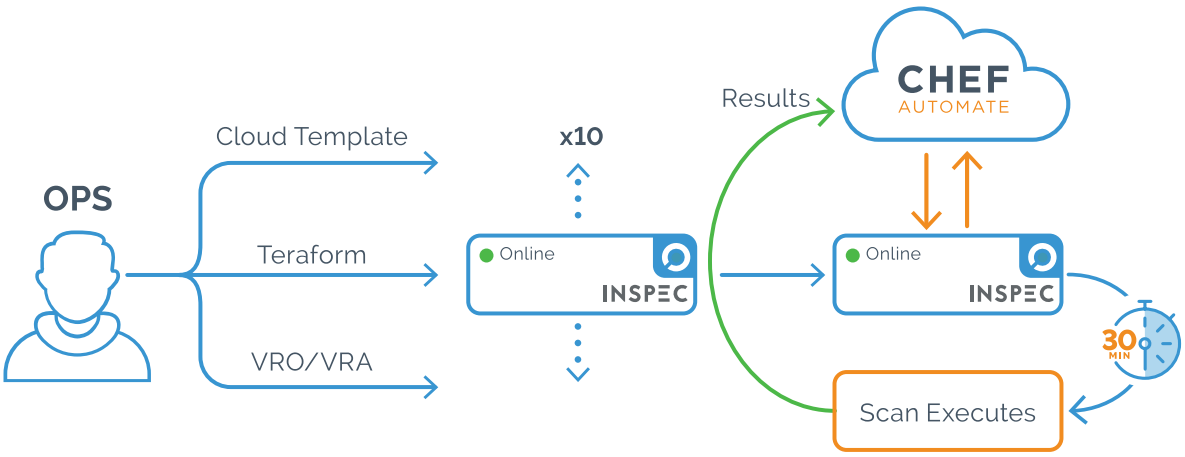
It's vital to assess the state of these systems as they come online, especially the nearer they are to production environments. InSpec can determine the infrastructure's compliance stance

at the earliest possible opportunity, addressing potential vulnerabilities before they can impact the businesses.

Step 1 - the operations unit trigger an infrastructure deployment using cloud templates, Terraform or VRO/VRA.

Step 2 - use a post deployment script to install the InSpec agent, or this may already be present and scheduled to run in a baked image.

Step 3 - the client authenticates with the Chef Automate platform, retrieves the GDPR profile, executes a local scan and reports the results back to the Chef Automate server.



Following the initial scan, the InSpec agent can continue to scan the environment on a schedule defined by the business. Scheduled scans that produce up-to-date results can help support audit readiness.

SOFTWARE DELIVERY

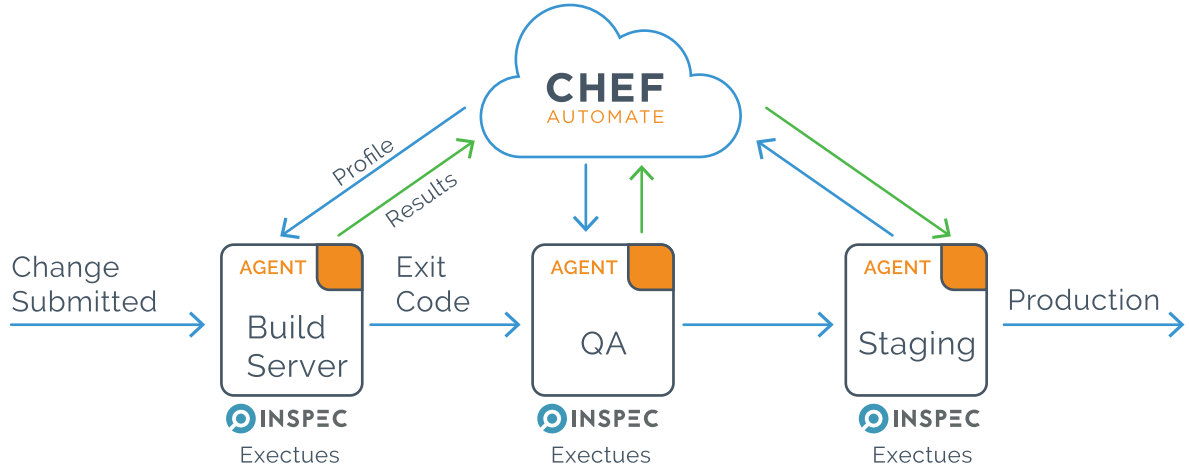
It is now common practise to build, test and deliver software using some sort of pipeline. Whether referred to as CI/CD or not, this is an increasingly common method to speed up the delivery and improve the quality of the products that businesses are shipping.

As changes are promoted through the environments in the software delivery pipelines, it is critically important to ensure that the changes do not impact the GDPR controls in place. InSpec has execution options that seamlessly integrate with existing task based pipelines.

Step 1 - define a task in the build pipeline that executes InSpec in each environment.

Step 2 - InSpec runs and retrieves the GDPR profile from Chef Automate, compiles and executes locally and produces an exit code based on the scan results.

Step 3 - If the exit code is a failure, the build stops and the scan result data is used to remediate the issue. If the exit code is a success, the build passes to the next environment and the change can be verified there too.



GDPR COMPLIANCE WITH AGILITY AND SPEED

When compliance is code, development and InfoSec teams can collaborate via pre-approved, easy to consume, automated processes that can be built into every part of the development cycle. With the new challenges GDPR presents, it's vital that DevOps organisations can extend this model into an approach where compliance is continuously assessed and remediations are continuously deployed.

By bringing the compliance data into the domain of the IT organisation, we can automate compliance as a stepping stone for greater ALDO engagement across the business. Compliance touches all areas, such as finance, HR and marketing, and tackling GDPR with InSpec and Chef Automate presents a unique opportunity to engage these business functions.

LEARN MORE

To find out more about implementing automated GDPR compliance in your organization, go to https://www.chef.io/gdpr

OR :
To find out more about implementing continuous compliance in your organization, go to https://www.chef.io/solutions/compliance/.