The road to GDPR compliance

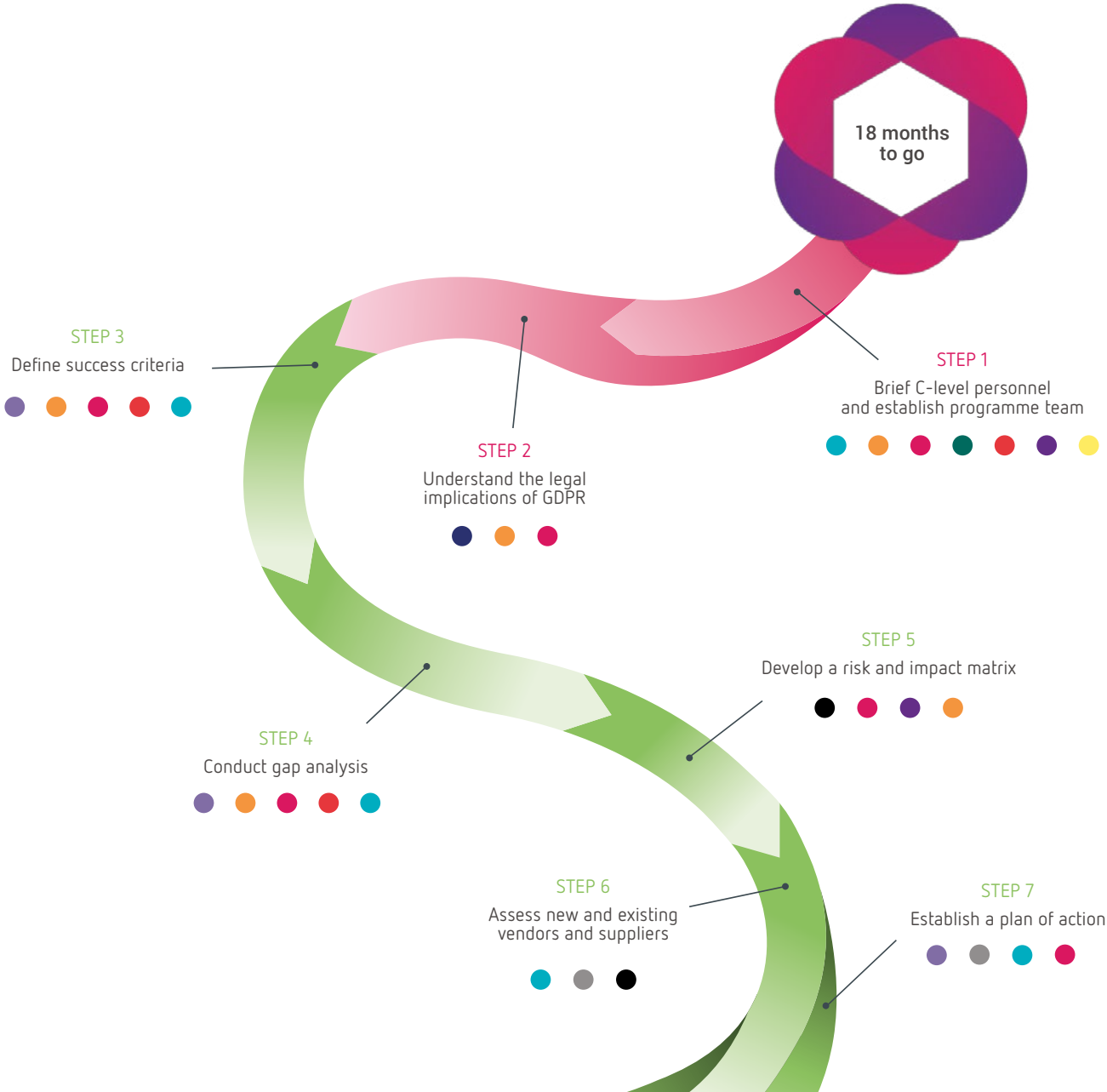
The countdown to compliance has begun. On 25 May 2018 the General Data Protection Regulation (GDPR) will be enforced in the UK and across the EU.

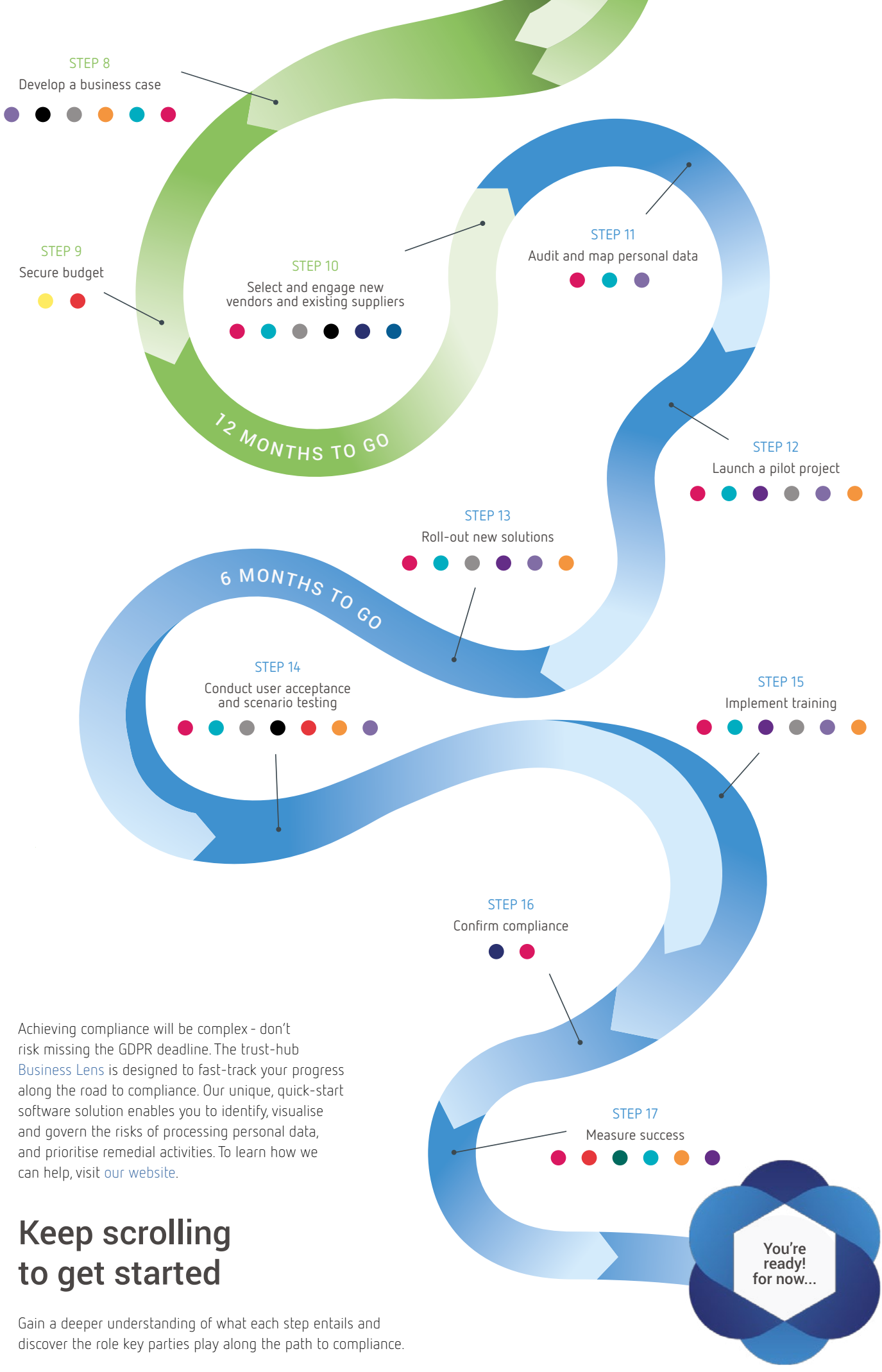
The Regulation introduces stringent requirements regarding the storage and protection of personal data and your staff, systems and processes will have to meet new standards if you're to avoid the threat of fines, litigation and reputational damage. Achieving compliance isn't a simple tick-box exercise either. The legal and regulatory landscape will continue to shift as GDPR takes effect, so ongoing risk management and flexible processes will be crucial if you're to remain on the right side of the law. Evolving customer and employee expectations must also be factored into the equation.

Achieving this degree of agility and control before May 2018 will be a challenge so it's important to get started immediately. Below, we've outlined the steps for a typical compliance programme - this framework is designed to help you develop and refine your own programme. It highlights the key stages of the process and explains where specific stakeholders need to be involved. We hope you find it useful.

KEY PARTIES

- The Board
- CEO
- COO
- CFO
- CIO
- CISO
- CTO
- CMO
- DPO
- Legal
- Head of Compliance
- Head of Digital
- Procurement





Achieving compliance will be complex - don't risk missing the GDPR deadline. The trust-hub Business Lens is designed to fast-track your progress along the road to compliance. Our unique, quick-start software solution enables you to identify, visualise and govern the risks of processing personal data, and prioritise remedial activities. To learn how we can help, visit our website.

Keep scrolling to get started

Gain a deeper understanding of what each step entails and discover the role key parties play along the path to compliance.

The GDPR compliance checklist

Phase A – Pre-programme

Step 1: Brief C-level personnel and establish programme team
Ensure C-level personnel understand that GDPR is a strategic issue and highlight the challenges and opportunities that may arise when aligning your business with the Regulation.

Next, establish a cross-functional team to manage the process and determine the budget and resources necessary to complete the programme successfully. It may be prudent to establish a senior-level steering team to oversee the programme and ensure it remains on track.

Step 2: Understand the legal implications of GDPR
GDPR introduces several new principles and requirements that are not included in the UK's Data Protection Act 1998 (DPA). To understand the legal implications of these changes it may be necessary to seek the advice of external specialists.

Phase B – Programme initiation and planning

Step 3: Define success criteria
Determine how you will measure the success of your GDPR compliance programme in the context of your business's strategic objectives and set key performance indicators (KPIs). These could include positive business and customer-related outcomes, such as cost savings achieved through the implementation of more efficient processes or improvements to customer experience.

Step 4: Conduct gap analysis
Compare your current approach to data protection against the requirements of GDPR to determine the size and scale of the challenge ahead of you. This may include a review of technologies, systems, processes, intelligence and supply chain relationships, as well an analysis of the types of personal data processed by your organisation.

Step 5: Develop a risk and impact matrix
Gauge the financial and reputational impact of a personal data breach on your business in the context of GDPR and calculate the potential cost of non-compliance with the Regulation. Next, determine the likelihood of these outcomes by identifying and ranking the causes of risk within your business. Finally, assess how you would currently manage a personal data breach to understand whether your existing procedures are adequate.

Step 6: Assess new and existing vendors and suppliers
Determine how new and existing vendors can help you bridge the gaps identified during the gap analysis process. If new solutions are necessary, conduct due diligence and seek quotations at this point.

Step 7: Establish a plan of action
Develop a detailed plan for programme execution with those who will need to be involved and agree key milestones.

Step 8: Develop a business case
Create a business case for GDPR compliance, aligning expected benefits to strategic business objectives. This document should include the benefits of achieving compliance, such as efficiency savings and improvements to customer experience, as well as costs, risks and challenges.

Step 9: Secure budget
Finalise budget and resource requirements and secure approval from senior stakeholders.

Step 10: Select and engage new vendors and existing suppliers
Complete the procurement of new solutions with both new and existing vendors.

The GDPR compliance checklist

Phase C – Programme execution

Step 11: Audit and map personal data
Identify the teams, systems and applications within your organisation that process, store and use personal data and determine precisely where this information resides. Next, classify this data by type and risk in accordance with GDPR.

Step 12: Launch a pilot project
Carry out a pilot project by rolling out new or updated solutions to a branch of your business, e.g. a single office. This will help you forecast the impact of a full-scale implementation

Step 13: Roll-out new solutions
Refine your plan based on what was learned during the pilot before rolling out solutions across your business and completing integration and technical testing. You may find that a phased rollout is more suited to your organisation.

Step 14: Conduct user acceptance and scenario testing
Conduct user acceptance testing to determine whether your new and updated solutions can handle specific tasks and challenges, and gather feedback on their initial performance. If possible, simulate a common personal data challenge to determine whether your processes match the capabilities of your solutions.

Step 15: Deliver training
Your Data Protection Officer (DPO) should deliver training to ensure your employees understand GDPR, its implications and their data privacy and protection obligations. It may be worth running this training programme concurrently with the pilot and rollout.

Step 16: Confirm compliance
Invite your DPO and legal advisers (internal and/or external) to review the efficacy of your compliance programme and present their findings.

Step 17: Measure success
Measure the success of the programme against pre-determined KPIs and targets, allowing for the fact that some benefits will only be realised after GDPR comes into effect.

You're ready! For now...
It will be necessary to continue to monitor the impact of GDPR on your business to ensure that the benefits of the programme are realised and no unexpected challenges arise. As data privacy is a subjective concept and GDPR is a dynamic Regulation, your business will need to constantly adapt to changes to the data protection landscape to ensure it remains compliant.

The trust-hub Business Lens can fast-track your progress on the road to compliance.
With the ability to track and govern the flow of personal data across your organisation you can put the right information in the right hands, when it's needed. This can help you make better decisions, simplify complex tasks and drive operations.

To learn more, please visit https://trust-hub.com/platform/

trust-hub is ISO27001 certified ™/© trust-hub 2016. All rights reserved