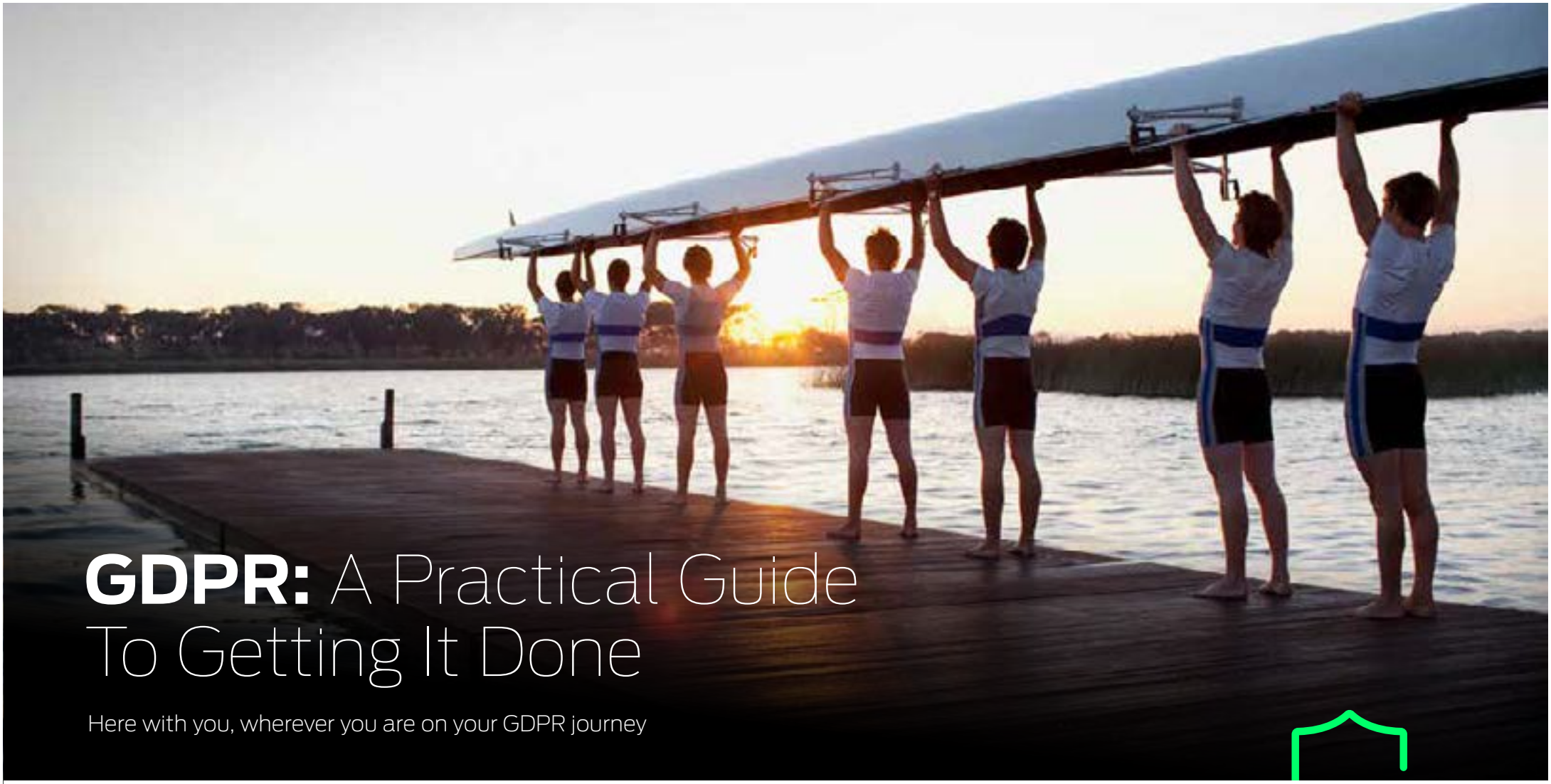


GDPR: A Practical Guide To Getting It Done

Here with you, wherever you are on your GDPR journey

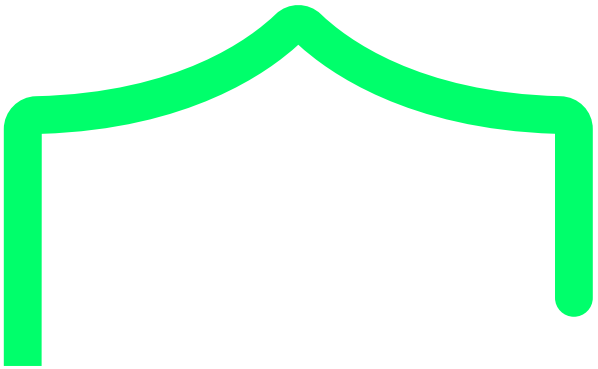
JUNIPER NETWORKS

BUILD MORE THAN A NETWORK.™

SECURITY

November 2017

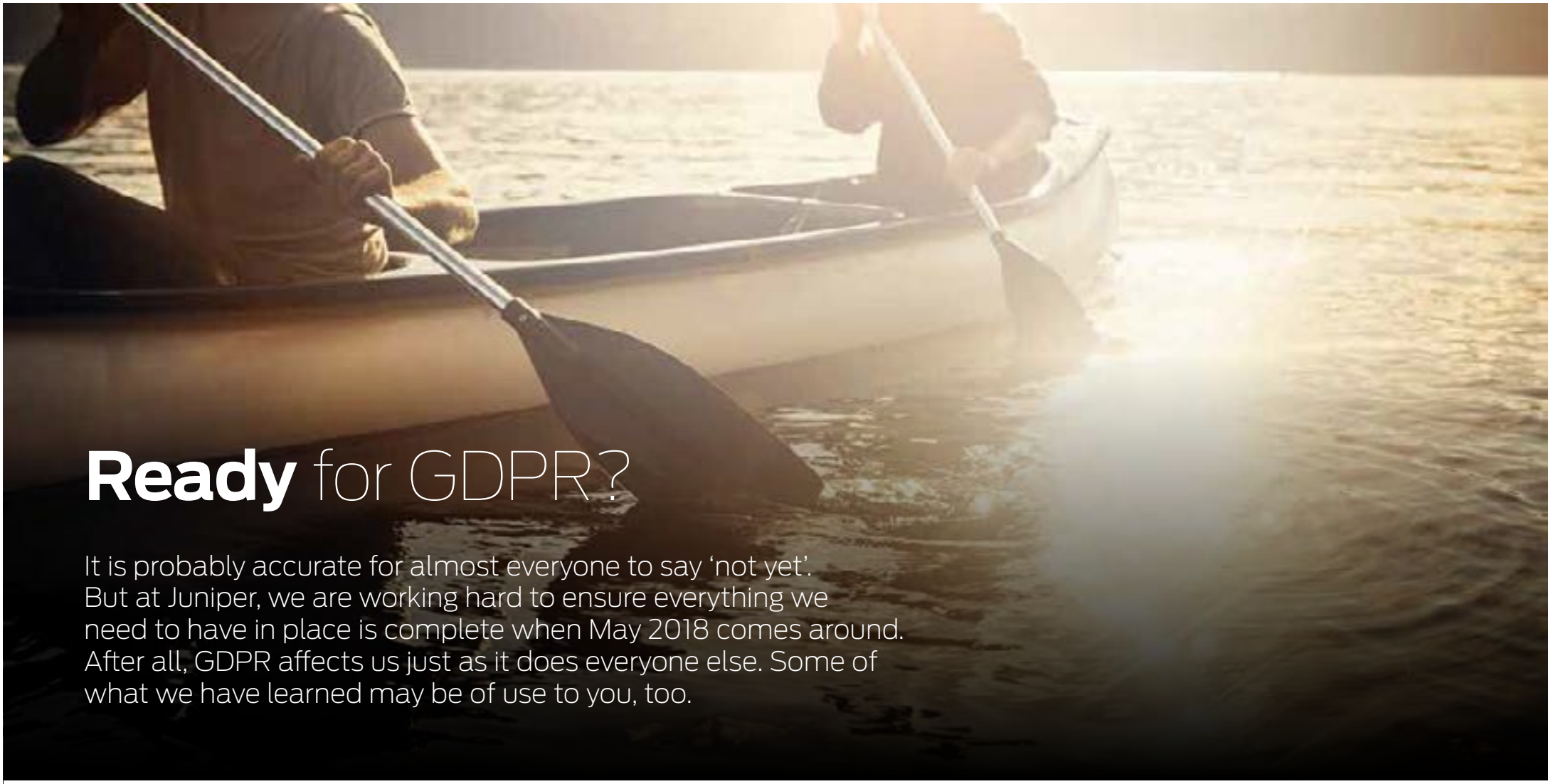
While General Data Protection Regulation (GDPR) compliance cannot be achieved with a one-stop product or solution, the data and applications you are required to protect and audit by GDPR are used by your network. Which is why the network, and network-based security, should be key factors in your GDPR planning.



By thinking carefully about data security and performance in relation to your network, you are better equipped to develop and enact meaningful policies, deploy effective threat detection and prevention strategies, and provide compliant audit reports.

Any enterprise, regardless of its geography, size or industry will need to be GDPR compliant from May 25th, 2018 onwards IF it is handling, managing or storing the personal data of EU citizens. So, as your first step on the journey to GDPR compliance, an intelligent, automated and secure network from Juniper Networks will probably be a smart step.

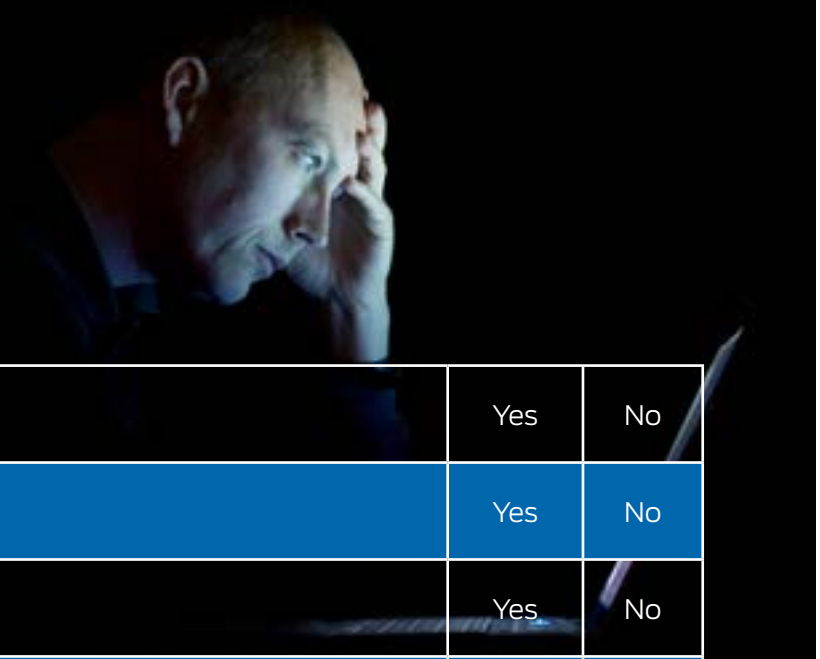
So, we hope as you join us on our journey, you'll pick up hints, tips and best practice ideas that help you to get your own organization in great shape for GDPR.



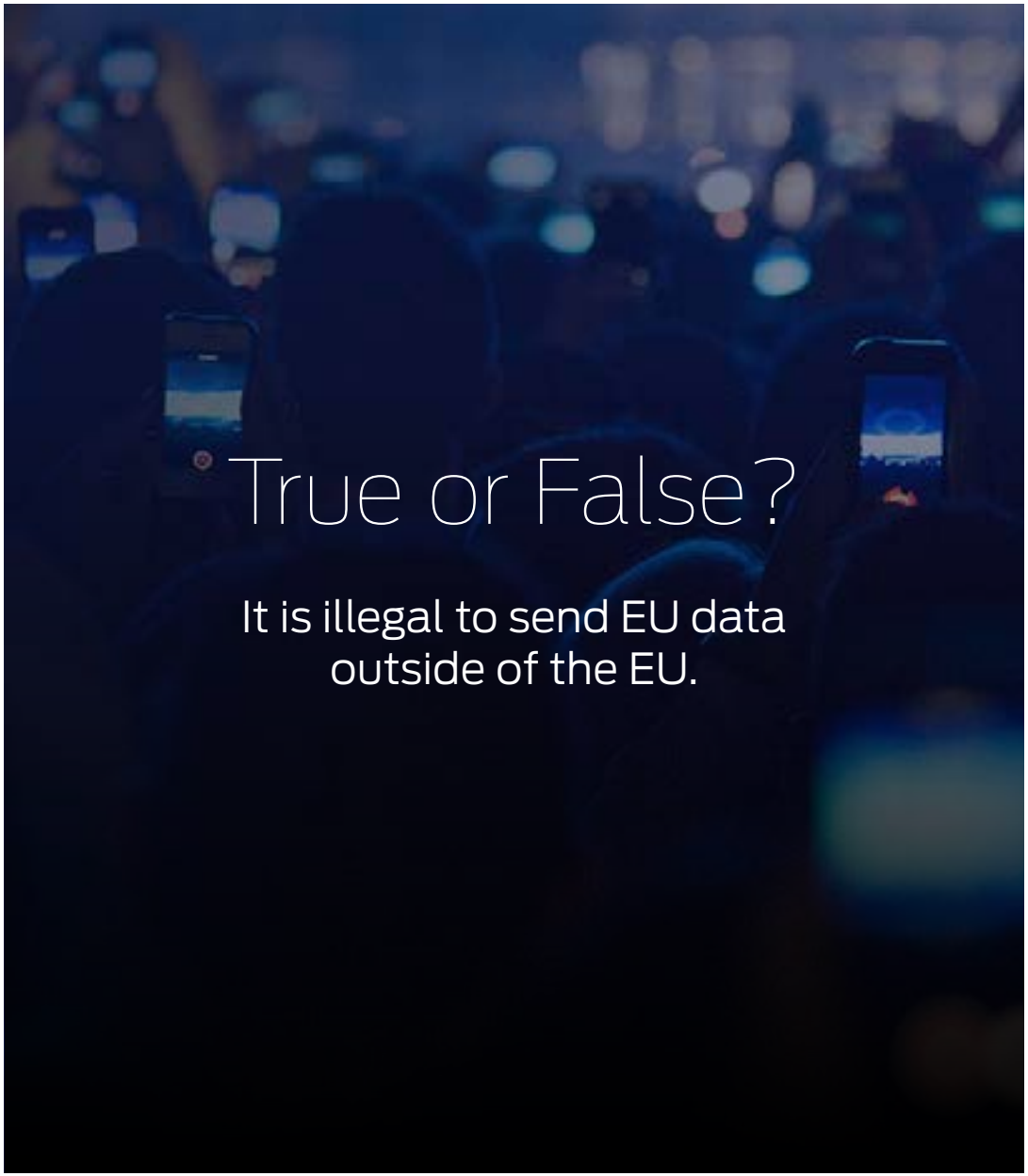
Ready for GDPR?

It is probably accurate for almost everyone to say ‘not yet’. But at Juniper, we are working hard to ensure everything we need to have in place is complete when May 2018 comes around. After all, GDPR affects us just as it does everyone else. Some of what we have learned may be of use to you, too.

Our plan is detailed further along in this document. It was shaped in part by asking ourselves some simple questions.

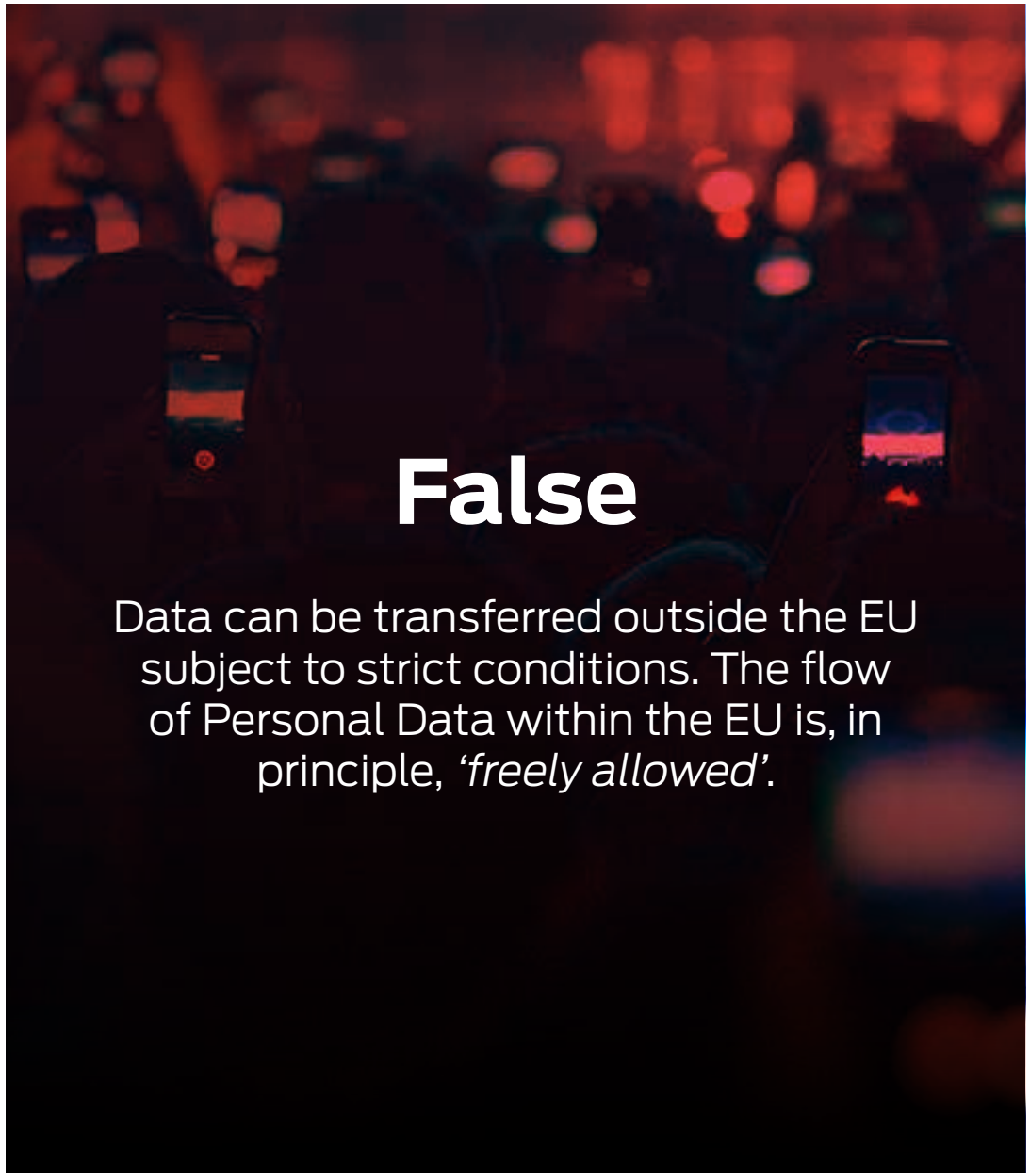


Do you know what personal data about individuals you process?	Yes	No
Do you know where it is and how it flows in the organization?	Yes	No
Do you consider security and privacy at network infrastructure and user levels?	Yes	No
Do you think 'user first' in your approach to security?	Yes	No
Have you reviewed your information risk management process for data privacy?	Yes	No
Have you reviewed your security controls against privacy requirements?	Yes	No
Do you have robust detection and monitoring processes?	Yes	No
Have you tested and implemented your response plans, including notification and external communication?	Yes	No



True or False?

It is illegal to send EU data outside of the EU.



False

Data can be transferred outside the EU subject to strict conditions. The flow of Personal Data within the EU is, in principle, *'freely allowed'*.

Understanding the Basics

At Juniper Networks, we are on a journey to GDPR just like you. We see it as an opportunity to embrace new standards in the processes, policies and management surrounding our data throughout its lifecycle – from consent and collection, through usage to storage.

The **Facts**

1. GDPR was proposed in January 2012 as a way to standardize the approach to data protection across all member EU states
2. Approved by EU states in 2016
3. Enforceable from May 25th, 2018
4. Affects all organizations processing personal data
5. Augments the protection of data for EU citizens no matter where it is stored. Ongoing compliance is, therefore, a necessary aspect of doing any business that involves handling EU citizen data, regardless of your global location

You probably will not be surprised to know that there is no 'silver bullet' product that you can install to ensure compliance. What's more, the GDPR compliance deadline of May 25th, 2018 should be viewed as a starting point, not an end goal.

So, read on to learn more about GDPR and the road to compliance. It is a journey about which we intend to share our progress between now and May 2018, so look out for more updates at www.juniperemea.net/GDPR

*"**Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Reference: EU General Data Protection Regulation (GDPR).

Like every other organization who handles the personal data of EU citizens – employees, partners, suppliers and customers – Juniper faces the GDPR compliance deadline of May 25th, 2018. We're evaluating our own processes and reviewing our own ability to understand, track, manage and protect that data effectively. And, as you might expect, we've started with our network.

The **Threat** of Non-Compliance

By now, of course, you are likely aware of the issues of non-compliance and the threat to organizations that do not meet the requirements of GDPR. You may have seen the headlines, such as:

A fine of **2%** of global revenue up to **€10m**

A fine of **4%** of global revenue up to **€20m**

These fines are real. It really could be the case that organizations are hit with heavy financial sanctions if found in contravention of GDPR requirements in the event of a data loss or breach (not to mention the potential impact on your brand).

To prevent the worst case from happening, it is advisable to have a clear audit trail within your organization that covers two aspects:

1. A demonstration of strong processes designed to ensure you are quickly aware of any data breach happening within your organization.
2. A clear outline of how you are addressing data breaches in your organization.

So, our suggestion would be:

1. Understand the framework and what's at stake for your organization
2. Put a robust plan in place to ensure you have good data hygiene for your customers and employees
3. Act on the plan in a way that you can document and so demonstrate compliance should a data breach arise
4. Secure your brand and, with it, the confidence your customers have in you maintaining their personal data

GDPR is not an EU issue, it is a non-negotiable global requirement

Any enterprise, regardless of its geography, size or industry vertical, will need to be GDPR compliant from May 25th, 2018 onwards if it is handling, managing or storing the personal data of EU citizens.

Who's Who in GDPR?

DATA CONTROLLERS
The person who is responsible for data, like a business or organization.

DATA PROCESSORS
May be the business or it may be outsourced to a third party provider or cloud application.

DATA SUBJECTS
This is every EU citizen to which the data refers.

DATA PROTECTION OFFICERS
Designated persons responsible for making sure the organization follows the new regulations. Must be a senior role to have impact.

Every organization will need to have a DPO, someone senior in the business who keeps informed about GDPR. This person may be dedicated within the business or is hired in as a service provider to fulfil that role. Every organization will have to make public who its DPD is.

STATE DATA PROTECTION SUPERVISORY AUTHORITY

Every EU country will have a designated supervisory authority to ensure the regulation is enforced equally within each country.

Every EU State Has A **Supervisory Authority**

This is replicated across EU member states.

Each state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offenses, etc.

SAs will cooperate with other SAs, for mutual assistance and joint operations.

Pan-EU businesses will have a single SA as their 'lead authority' based on the location of EU headquarters.

Third Parties Handling Your Data

Remember, you remain accountable for any breach that occurs to the data you own or process irrespective of further third parties that might be engaged by you. Your third-party service provider contracts have to reflect the EU model clauses to ensure sufficient protection.

GDPR **Scope**

You need to understand and define the type of data you record, and why you record it

Consider whether you need it, what its purpose is and why you recorded it

You need to identify a lawful basis before you can process personal data

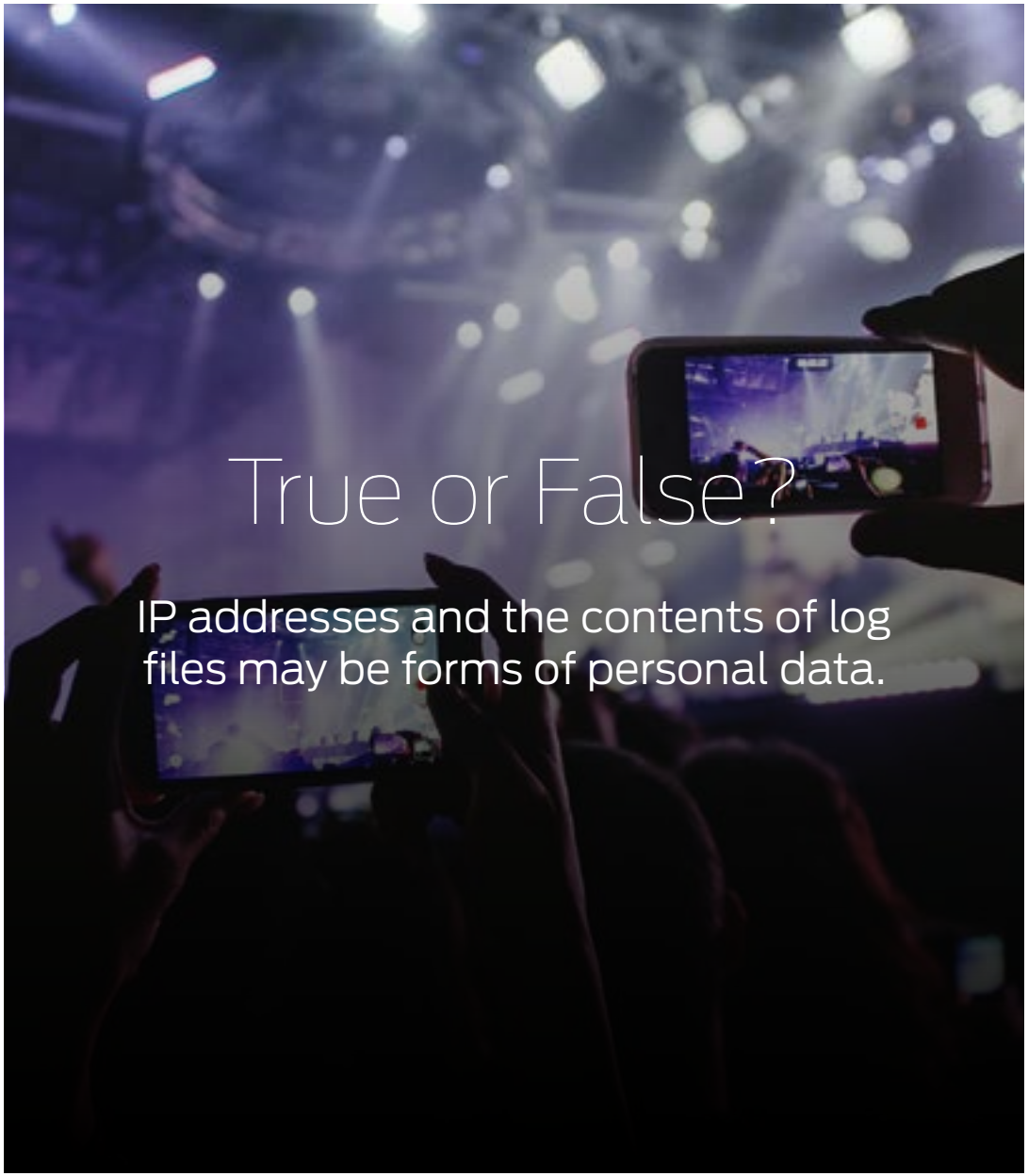
The lawfulness of data processing conditions includes, but is not limited, to the consent of the data subject

Security controls need to be defined, implemented and measured to ensure compliance

Here, you have to demonstrate the security controls you have in place to secure your data inside and outside of your business, including how those controls have been implemented and enforced

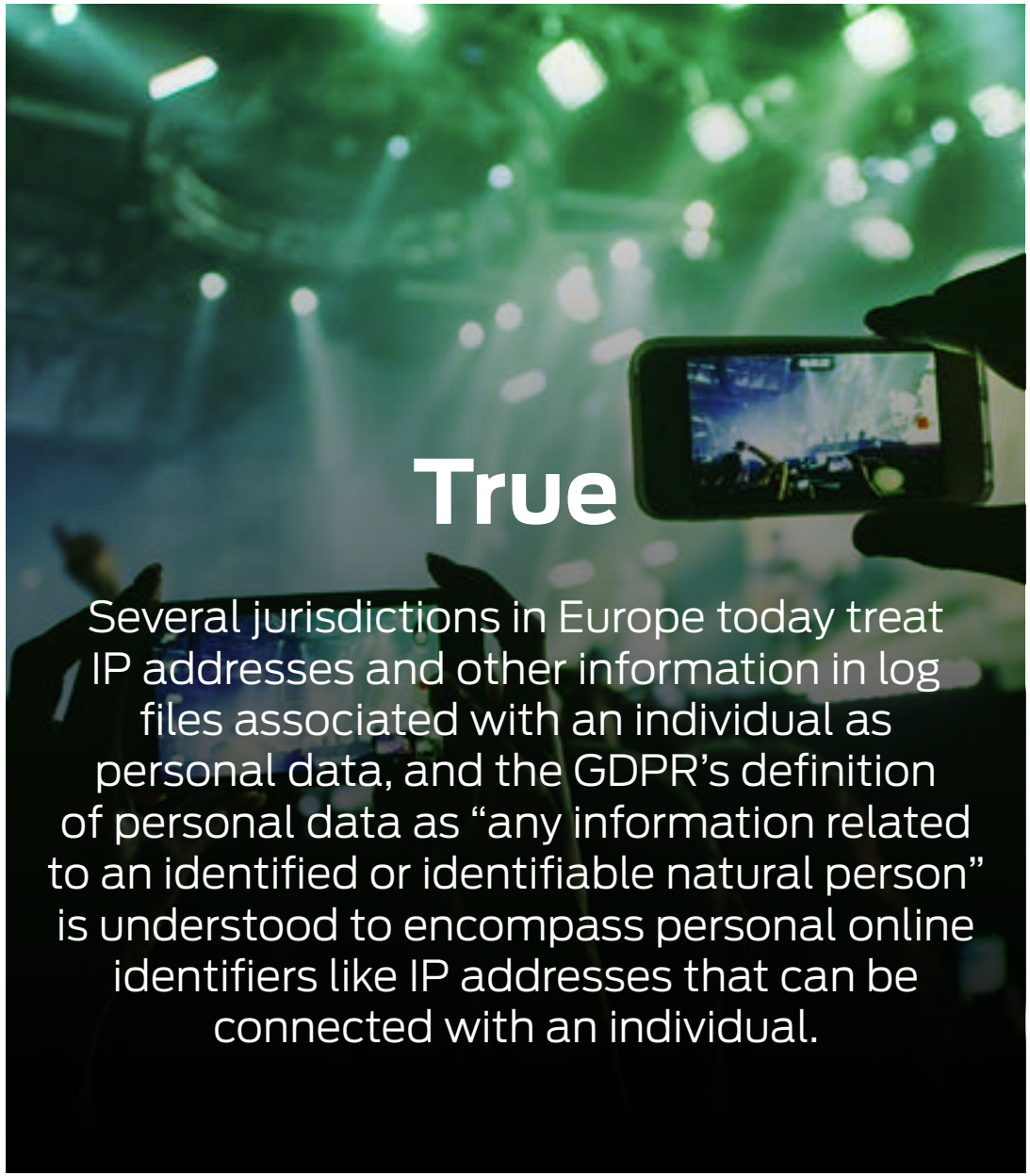
Privacy needs to be embedded into the design of your approach, from capture, storage, transmission and processing of the data

Look at how you capture data, how you process it, who processes it, who accesses it, the tools you use to facilitate this, how you secure it from end to end and ensure you can articulate this to auditors



True or False?

IP addresses and the contents of log files may be forms of personal data.

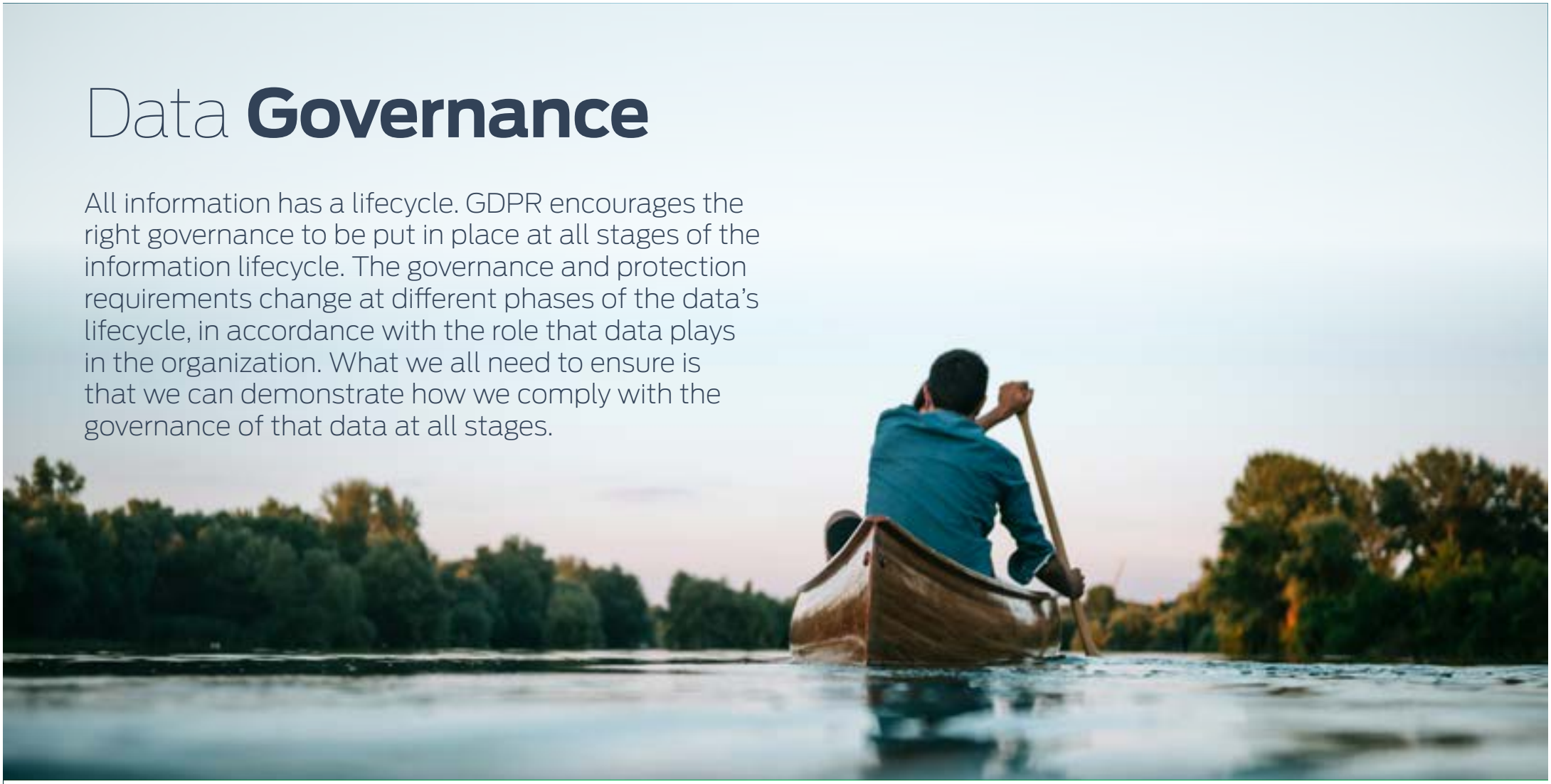


True

Several jurisdictions in Europe today treat IP addresses and other information in log files associated with an individual as personal data, and the GDPR's definition of personal data as "any information related to an identified or identifiable natural person" is understood to encompass personal online identifiers like IP addresses that can be connected with an individual.

Data **Governance**

All information has a lifecycle. GDPR encourages the right governance to be put in place at all stages of the information lifecycle. The governance and protection requirements change at different phases of the data's lifecycle, in accordance with the role that data plays in the organization. What we all need to ensure is that we can demonstrate how we comply with the governance of that data at all stages.



The **Lifecycle**

DATA COLLECTION

Fairly and lawfully
With consent
Relevance
Types of data

PERMISSION APPLIES TO:

Specific data
Specific purpose
Notified changes

MANAGEMENT OF:

Access controls
Right to edit, rectify
Data destruction
Data transfers
Rules, controls, audits

STORE

Duration
Types of data

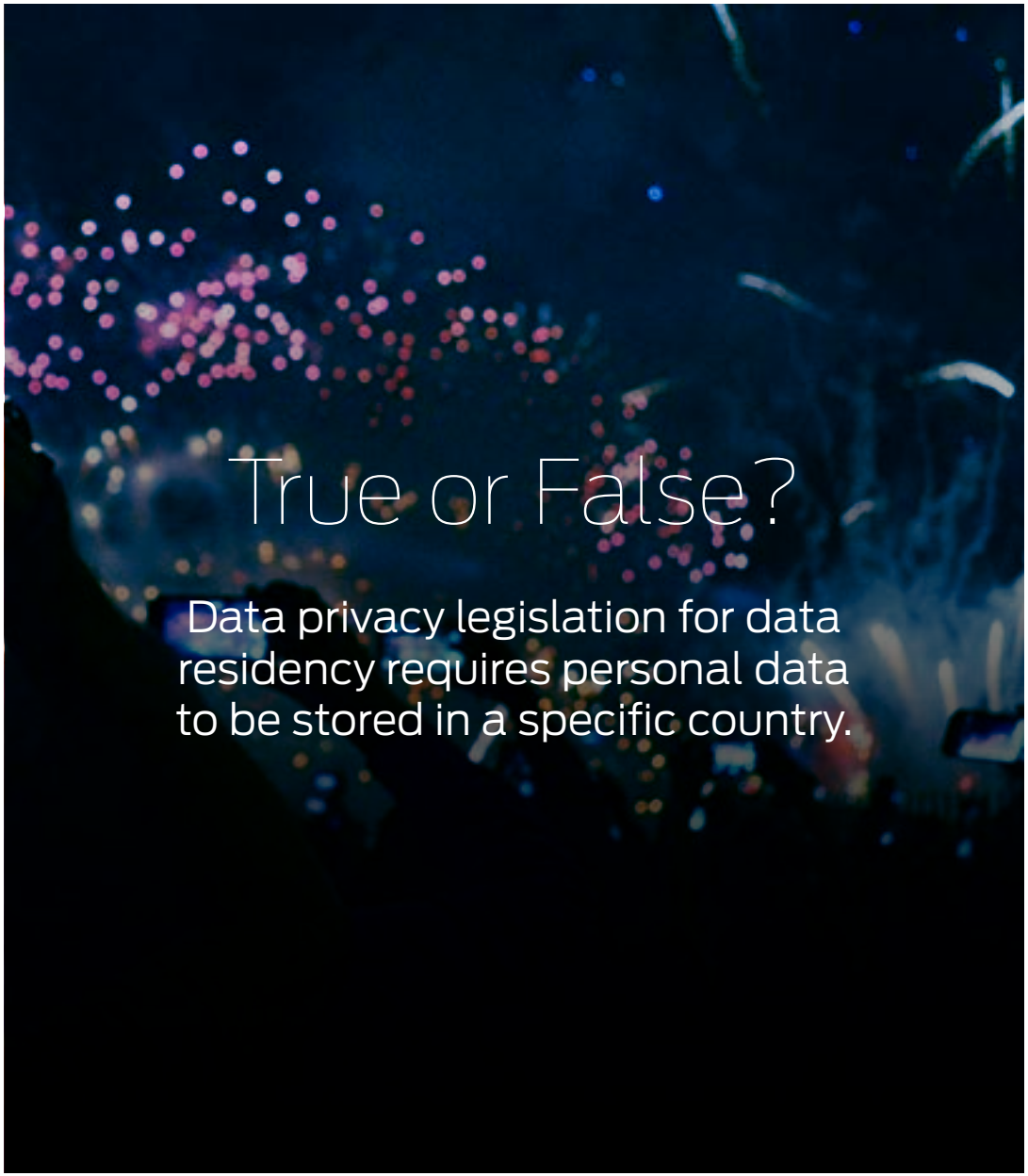
SECURE

People
Process
Technology
Data loss

Reviewing Your Privacy Standards

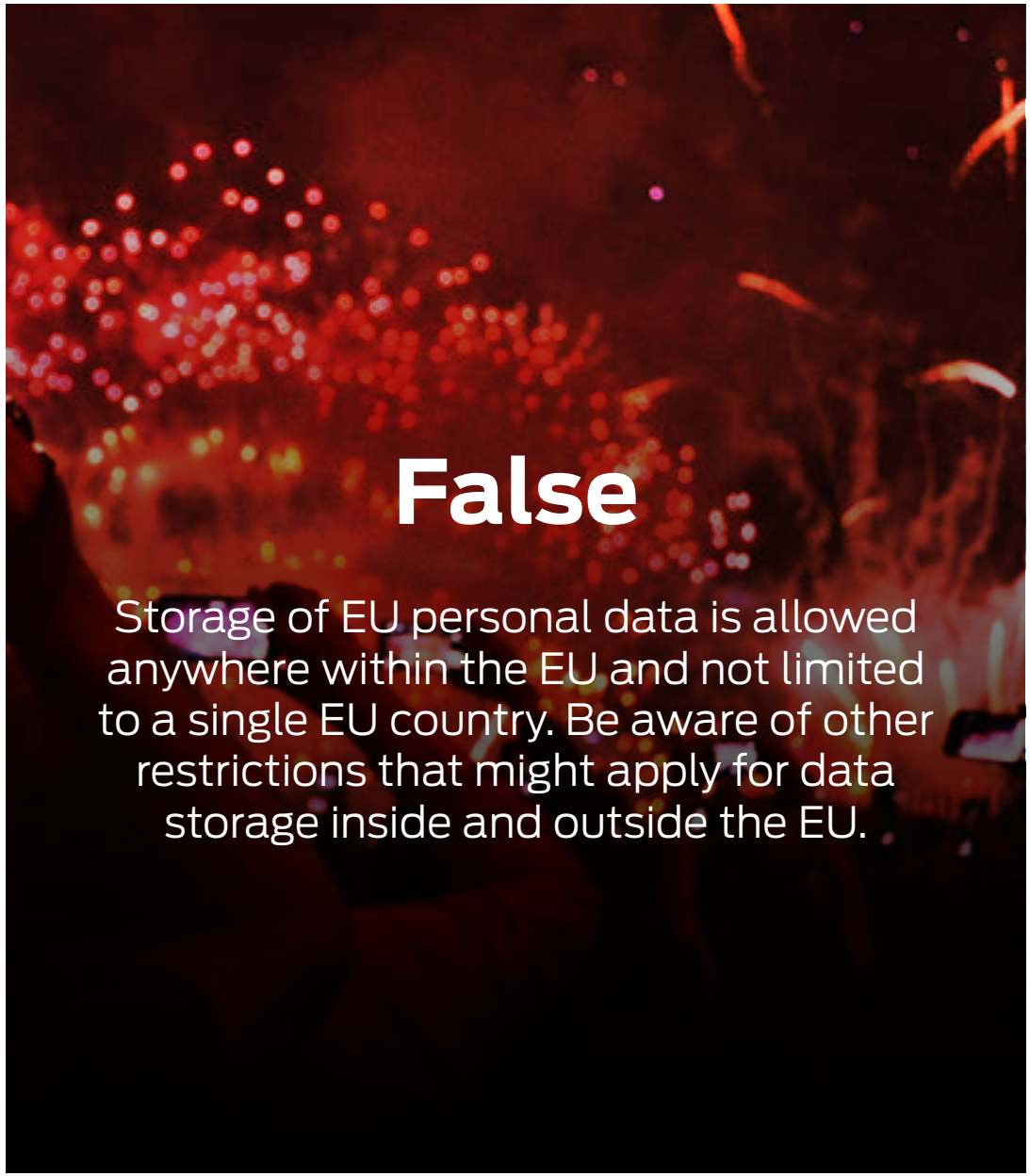
Under GDPR there are some **additional** things you will have to tell people. For example, you will need to explain your **reasons for collecting** the data, your **data retention periods,** and that **individuals have a right to complain** to the regulator if they think there is a problem with the way you are handling their data.

Note that GDPR requires the information to be provided in concise, **easy to understand** and clear language.



True or False?

Data privacy legislation for data residency requires personal data to be stored in a specific country.

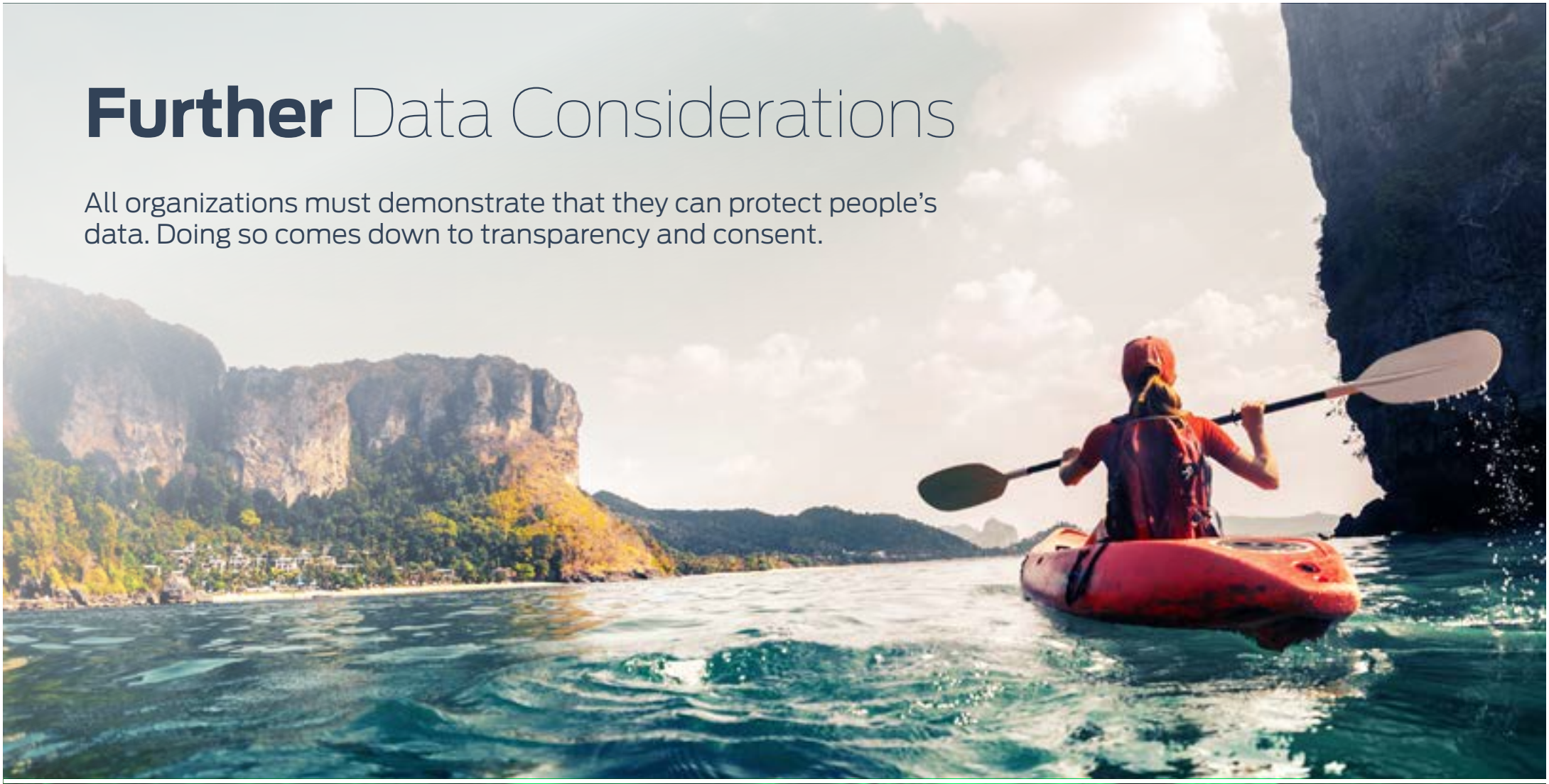


False

Storage of EU personal data is allowed anywhere within the EU and not limited to a single EU country. Be aware of other restrictions that might apply for data storage inside and outside the EU.

Further Data Considerations

All organizations must demonstrate that they can protect people's data. Doing so comes down to transparency and consent.



Transparency and Consent

Articulate what data you are capturing and why you want it.

Demonstrate approval and consent that data you hold can be used in accordance with how you have stated that data will be used.

Information on how personal data will be used must be provided to individuals in a clear and concise manner.

Individuals must grant permission for use and storage of personal data.

Did You Know?

Regulated data

The definitions of *'Personal Data'* and *'Sensitive Data'* have been expanded in GDPR. For instance, the former now includes online identifiers like IP addresses collected from your digital interactions, while the latter now includes genetic and biometric data.

Example: Healthcare providers must consider this when planning the scope of GDPR.

Children and Consent

For children under 13, parental consent is required to process and store data.

For children between 13 and 15, member states can set own rules for consent to use their personal data.

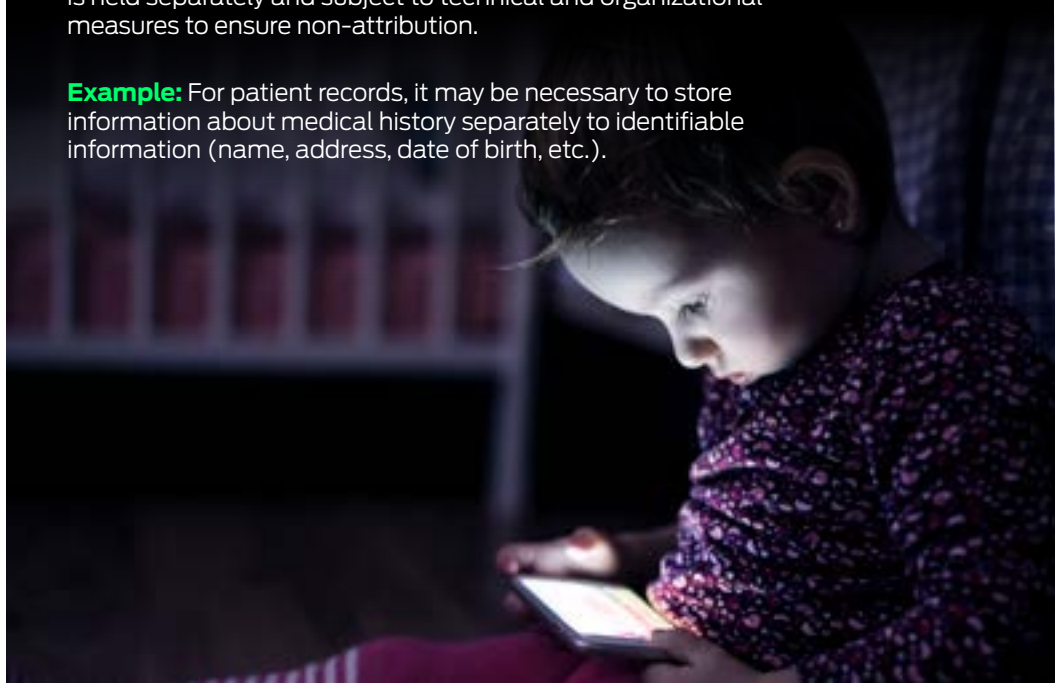
If a member state does not set rules, then consent is required for all children up to age 16.

Did You Know?

Pseudonymization

Information that allows data to be attributed to a specific person is held separately and subject to technical and organizational measures to ensure non-attribution.

Example: For patient records, it may be necessary to store information about medical history separately to identifiable information (name, address, date of birth, etc.).



Recognizing the **Rights** of the Individual

An important aspect of GDPR is the augmented rights of individuals. The rights individuals will enjoy under the GDPR are generally the same as those under current regulations but clarified and partly extended. GDPR also introduces new rights for individuals. Rights under the GDPR are:

- The right to be informed;
- The right to access;
- The right to rectification;
- The right to erase;
- The right to restrict processing;
- The right to data portability;
- The right to object, and
- Rights in relation to automated decision making and profiling.

Dealing with **Requests to Access Data**

The EU rules for dealing with data access requests by individuals have been enhanced under GDPR. You will **not be able to charge** for complying with a standard request and have to deliver the information **within a month**.

You can refuse to respond to a data subject access request if it is manifestly unfounded or excessive. You could also charge for such requests. But, if you want to refuse a request, you will need to explain to the individual in detail why the request is refused. It is advisable to establish clear and objective criteria to define whether a request is unfounded or excessive. Consult the information website of your data protection authority for examples and guidance.

If your organization handles a large volume of access requests, you could save a **great deal of administrative cost** if you can develop systems that allow people to access their information easily **online.** Organizations should consider conducting a cost/benefit analysis of providing online access.

Dealing with **Data Breaches**

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. The GDPR will bring in a duty on all businesses to provide notification of certain data breaches to the Supervisory Authorities and individuals. This is new to many organizations.

Article 33 of the GDPR sets out a single data breach notification requirement designed to be applicable across the EU. In accordance with this Article, notifiable breaches have to be reported to the relevant supervisory authority for your organization generally **within 72 hours of learning about the breach.**

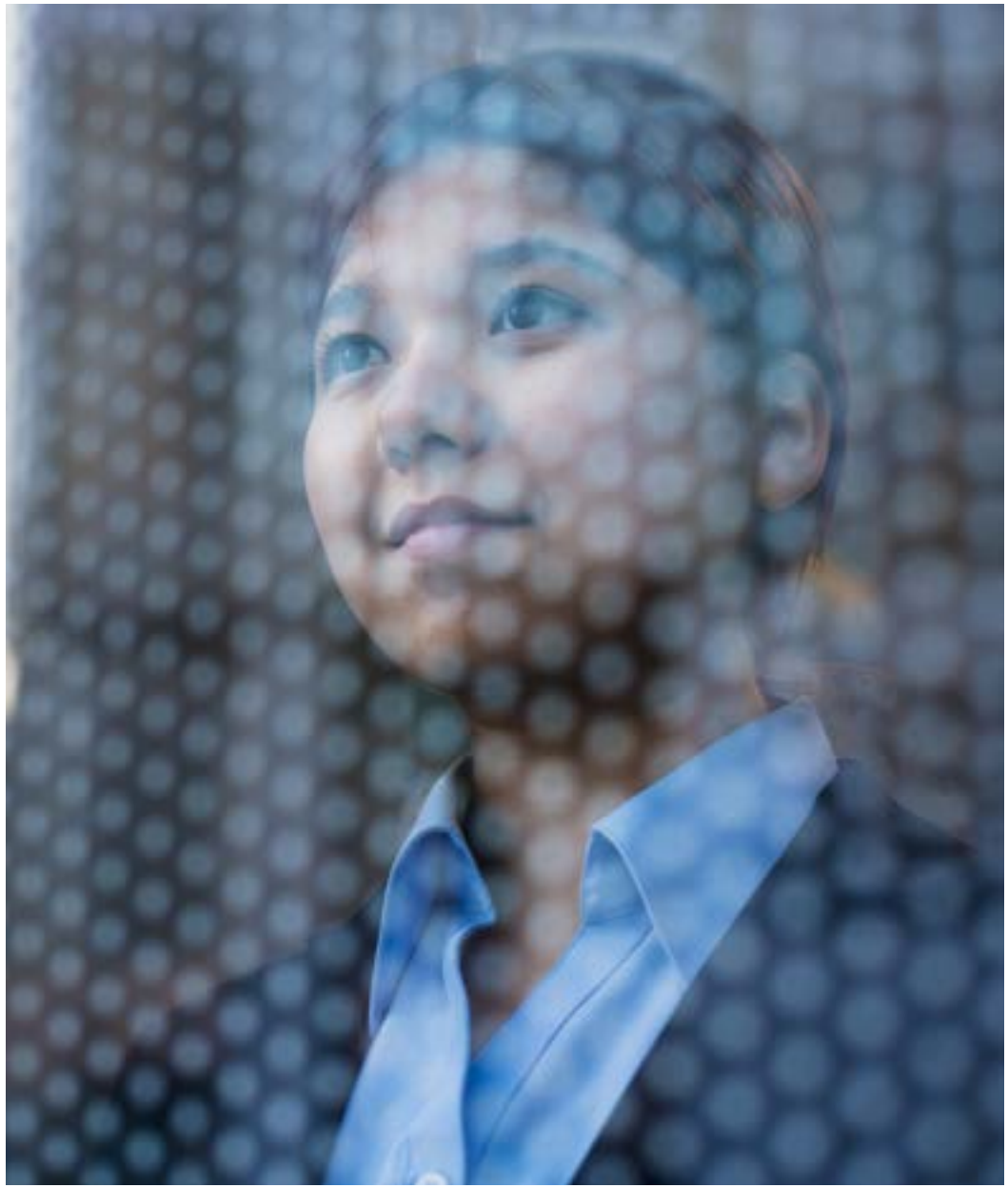
Article 34 requires you to notify data subjects of breaches "[w]hen the personal data breach is likely to result in a high risk [to] the rights and freedoms of individuals" and must notify data subjects of the breach "without undue delay." You might be released from that obligation if your organization has implemented appropriate technical and organizational measures, you have taken appropriate risk mitigation measures after the breach occurred and the efforts to inform the affected individual would be disproportional.

Four Stages to Juniper Compliance

At Juniper, like many organizations, we are actively venturing along a path to GDPR. Given that every organization is unique, you will probably establish your own approach to this challenge. But, to help you along the way, there are four stages that you may wish to consider within the planning and activation of your own GDPR journey.

Stage 1A:
Program and Team

In this first stage process, there are two distinct phases. The first of these is about identifying key individuals within your organization who can progress GDPR compliance efforts, identifying the data and processes in place to achieve compliance, and just as importantly, remaining compliant.



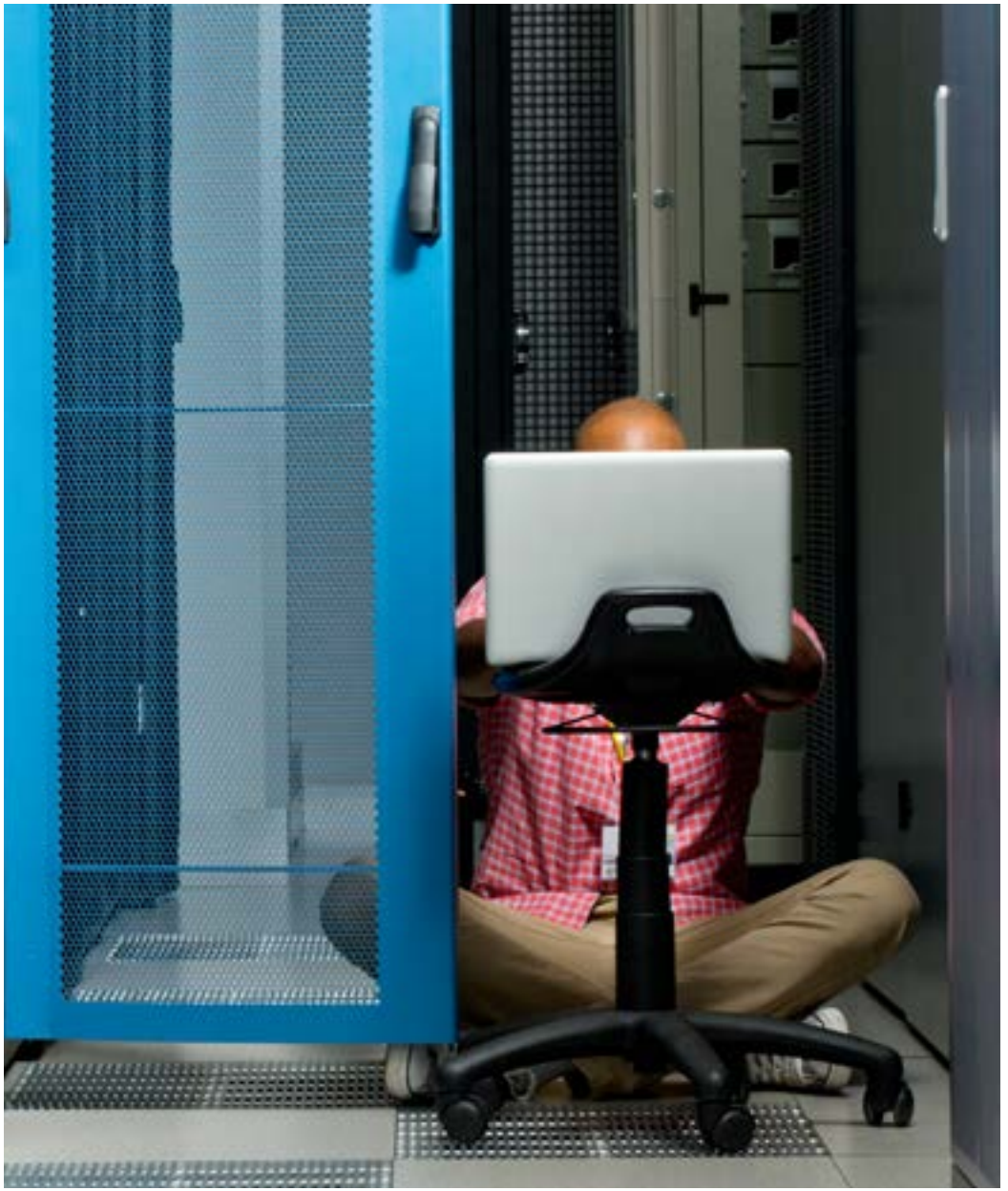
Stage 1A: Actions

1. Identification of key stakeholders within your organization who will be responsible for progress towards GDPR compliance and beyond, and of course, key influencers and communicators whose support is required.

GDPR affects many aspects of the business. As such, depending on your organizational complexity, it may require dedicated resource to ensure it gets the prioritization it needs. This may, of course, include a Data Protection Officer (DPO) (see page 10) and a Project Manager dedicated to the mission of preparing for GDPR, running a task force made up of resources from around your organization.

Consider the touchpoints across your operation that might deal, or at least come into contact, with personal data. This can encompass your product divisions, HR, finance, legal, marketing, communications, sales, IT and customer service operations. The leaders of all these functional domains in your organization should be briefed to ensure they understand the implications of GDPR. This ensures that the individuals assigned to execute necessary steps on your road to compliance have senior management support and are empowered to implement necessary changes.

Individuals will be accountable for the completion of actions within their field of expertise or part of the organization, so you need to ensure that they are empowered and, depending on the impact of GDPR on your organization, are supported by a project manager, ensuring communication, engagement and adherence to timelines.



2. Allocation of resources and budgets, where applicable.

Do not underestimate the number or resources and the budget that can be bound by an appropriate implementation of GDPR.
Of course, this will differ from organization to organization, but a starting point here is to draft a business case to present to your leadership team focusing on:

FINANCIAL APPRAISAL

Reflects forecasted project cost and breakdown of capital and operational expenditure items

SENSITIVITY ANALYSIS

Concerns the risk of not achieving GDPR compliance. Consider also the potential impact on outcomes that are based on uncertain values

BENEFITS AND LIMITATIONS

Describe the financial and non-financial benefits. The purpose is to explain why you need to be GDPR compliant

SCOPE, IMPACT, AND INTERDEPENDENCIES

Describe the work needed to deliver GDPR; the functions affected; and interdependencies with other projects

PURCHASING STRATEGY

This section describes how GDPR compliance needs to be financed (if at all) and whether solutions that require a financial outlay are a buy, lease, or outsource decision

PROJECT GOVERNANCE

This section details roles and responsibilities (the project team and stakeholders), the project tolerances, review points, and how decisions are made.

PROGRESS REPORTING

Finally, the business case should define how progress towards GDPR is recorded and how the project team updates others on performance and progress

3. Collection of existing policies and procedures (incl. training)

Another key element of this initial stage is to identify the policies and procedures in place already. This allows you to identify how they compare to the new, more stringent requirements for GDPR and to ensure gaps are identified in order to close them in time for the May 2018 deadline. Considerations here could encompass the following:

- Is there a documented procedure to identify and manage a data breach, should one occur today? Would you be prepared for the 72 hours notification requirement?
- Is there a procedure in place should a data subject ask to be removed from your systems or to access their own personal data? How would you comply with these requests?
- How are you currently collecting data, and what notices do you have in place for the data subject to understand how that data is being used? Furthermore, are you certain of the legal basis for the collection and use of the data?

4. Generation/creation/collection of relevant documentation (data map, workflow overview, data classification) to undertake data inventory and data flow analyses, risk assessments and gap analyses.

Knowing what data you have flowing across your extended network, how it is behaving, where it is in real-time, which threats it is facing, how your security solutions are performing, and how to defend your network elements and data in real-time, are fundamental building blocks in any successful, sustainable GDPR compliance process.

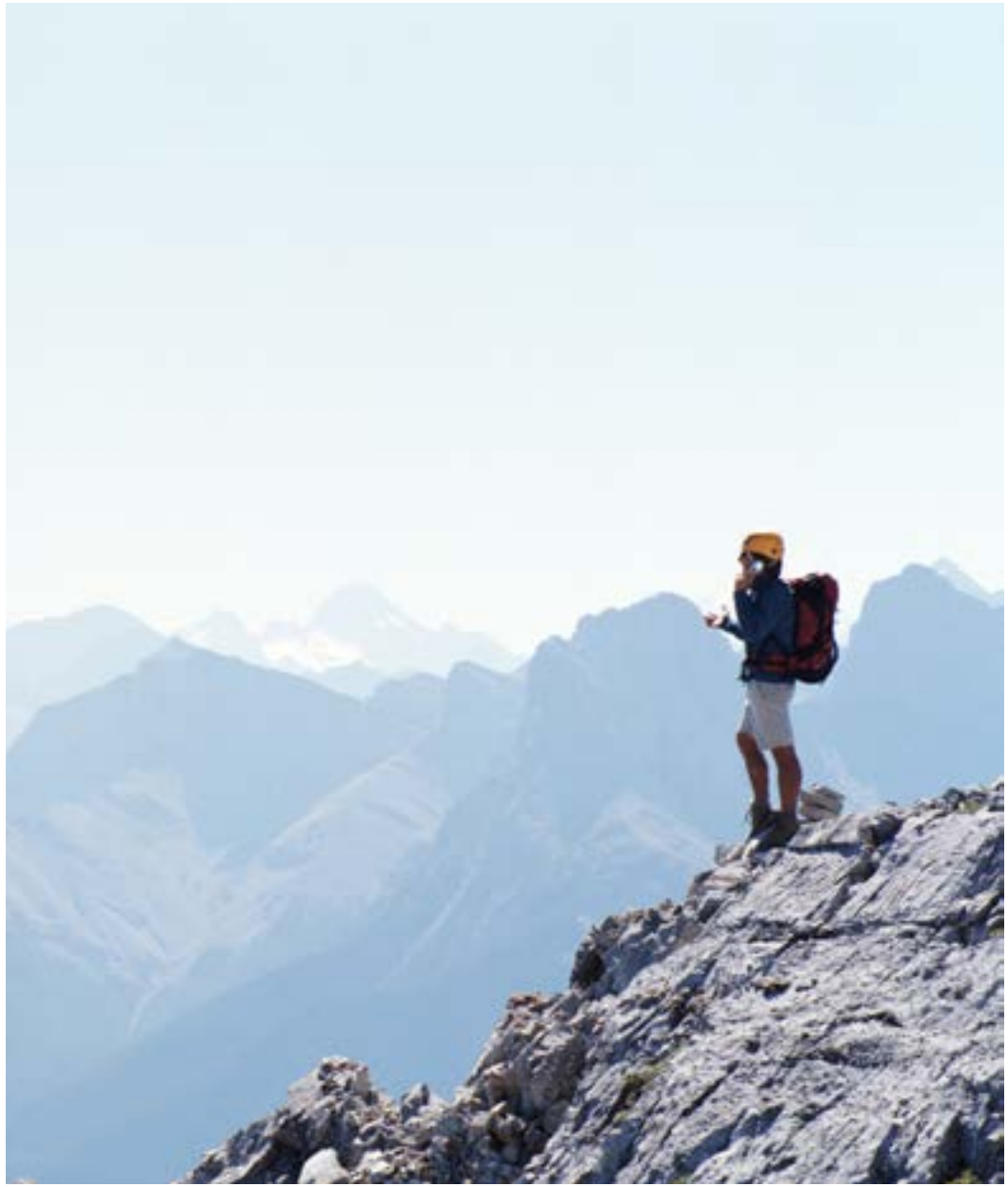
With high volumes of data constantly in flight, a technology-led approach to get a handle on the data that exists around your organization is likely the preferable approach. Consider, though, that there is no single 'GDPR' solution that will fit every organizational requirement. At Juniper, we've partly tackled this in a straight-forward way – together with external GDPR matter experts we have developed a questionnaire determining which data are collected, by whom, on which bases, for how long this are stored, how they are used, which processes and policies apply to ensure governance and which actions are taken in case of an irregularity. This questionnaire has been shared with appointed persons in the relevant functions at Juniper.

Of course, the use of personal data differs across departments, so it is important any questions asked at this stage are tailored to individual departments. It is also important that questions asked across functions are presented to people with the necessary insight to provide comprehensive answers.

Consider too that this process should also apply to data that travels across to third-party service providers and data recipients, such as websites, apps, HR, payroll, compliance, customer service and support, marketing, commercial and professional services.

Stage 1B: Risk Assessment and Creation of Internal Awareness

The second phase of stage one is about understanding the procedures and processes required in place by May 2018 and beyond. Having a baseline understanding of how your network and data normally behave day-to-day enables you to create and enforce effective detection and protection policies.



Stage 1B: Actions to Consider

Undertake a comprehensive assessment, providing:

a systematic description of data processing operations and purpose;

an assessment of its necessity and proportionality;

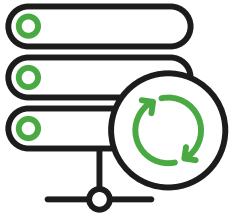
an assessment of risk associated with the data processing;

measures needed to address the risk.

Have in mind that you might be obliged to provide a Data Protection Impact Assessment as set forth under Article 35 of GDPR.

This is how Juniper has delivered this...

Create a summary of data necessity: reasons for its retention (to include anonymization and pseudonymization, if required), and, where applicable, its disposal.



Formulate an assessment of data integrity and control (which is likely to change through the information lifecycle in terms of authorization, completeness and accuracy). We've published a blog about the lifecycle of data, which you can find here.

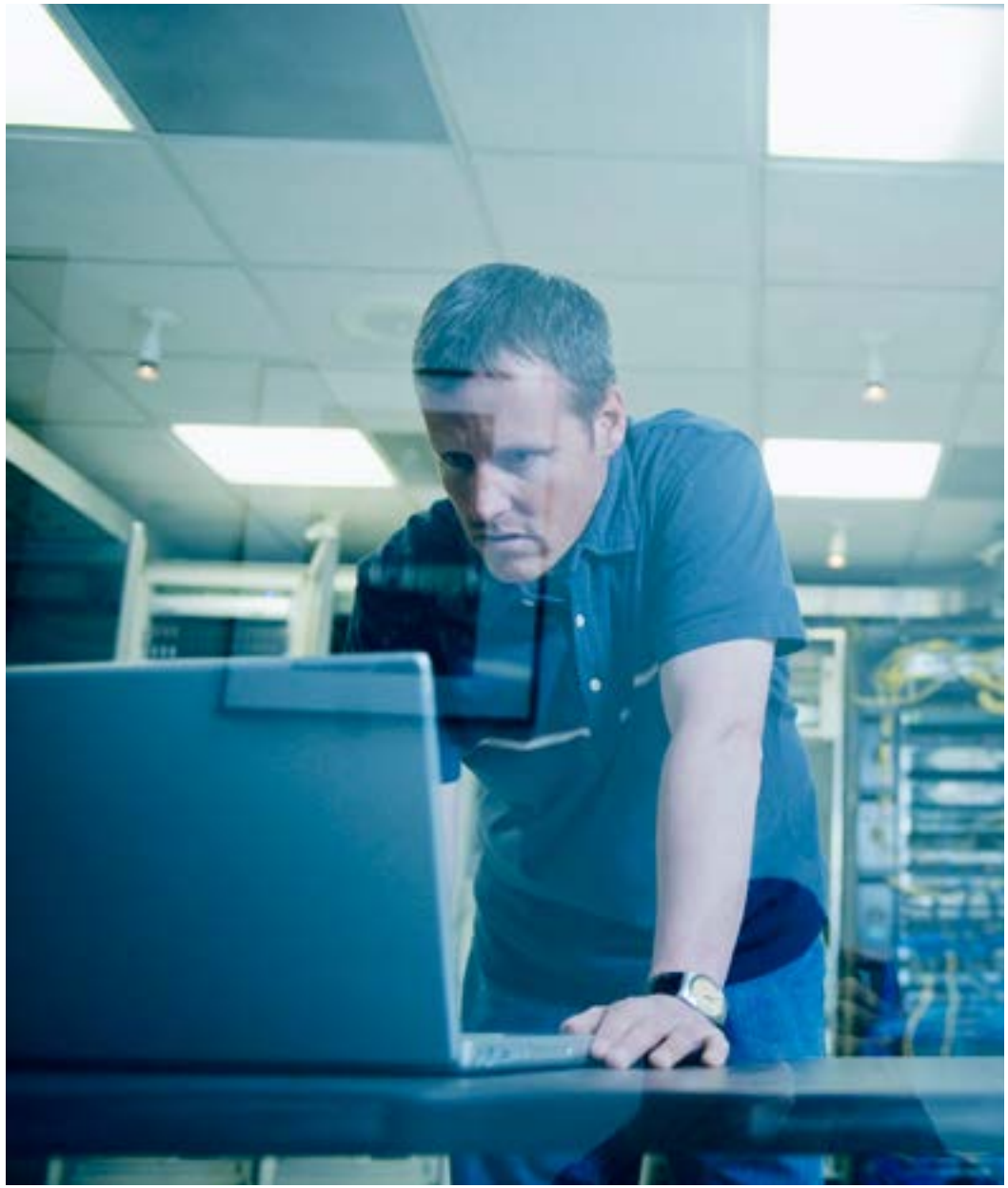
Implementation of a privacy shield to ensure all steps are taken to mitigate the risk of data breaches from within the organization and, of course, from outside threats. This is where the security of your data becomes your biggest consideration. Protection from data breaches, both inside and outside of the business, is a huge issue for all organizations, but the financial and reputational risk of such an event in a GDPR compliance climate makes this a top priority.

Do You Have a Risk Register?

An organizational Risk Register contains information about identified risks, analysis of risk severity and evaluations of the possible solutions to be applied. Presenting this in a spreadsheet is often the easiest way to manage things, so that key information can be found and applied quickly and easily.

Stage 2: Design Operational Controls

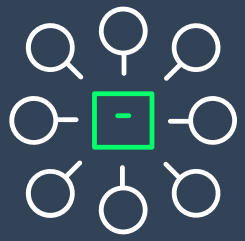
Providing effective security measures for the personal data your organization owns or processes is an important element of GDPR compliance, but it is just one element. A holistic approach to data's dynamic value, its changing status over a lifecycle, its overall behavior and its known normal characteristics can all provide invaluable, actionable insight. Coupled with effective, integrated security measures, we recommend this shapes and evolves your approach to data handling, which will lead to a much smoother and consistent road to GDPR compliance for the long term.



Some Key Challenges When Implementing GDPR are:

CONSENT REQUIREMENT:

Understand the consent that is assigned to data you hold and data you will collect in the future and ensure that your processes and tools reflect the necessary requirements re: information explicitly, and the possibility to withdraw. This might require substantial changes to the processes and tools you have in place today.



THIRD-PARTY ENGAGEMENT:

Part of your obligation under the GDPR is to ensure that third parties you are engaging in the handling of personal data are adhering to the GDPR. You have to review the existing contracts and put in place effective control measures for third-party management across your supply chain.

ACTIONS ON DATA BREACH:

Remember, you might have just 72 hours to report a data breach incident, so it's imperative to be running the right security solutions that prevent these from happening, but also inform you quickly in the event of it occuring.

Stage 2: Actions:

Consider solutions that help you to manage, monitor, protect and report your data flows and network behavior effectively. These should be solutions that help to enact, enforce and document processes consistently, solutions that help to reduce risk and increase visibility at the heart of your IT infrastructure, where key data resides and where all attacks are **therefore focused.**

ADDRESS SECURITY GAPS
(e.g. human error leading to data leakage, manipulation, unauthorized use, data transition, data encryption)

REVIEW EXISTING SOFTWARE, APPLICATIONS AND DATABASES IN CONTEXT OF THE FOLLOWING ASPECTS:

DESIGN OPERATIONAL CONTROLS
including technology but also staffing and organization

Data protection by design and default

Data minimization

Accuracy

Storage limitation/deletion

Data portability

Stage 3:
Manage and Enhance Operational Controls

At stage three, you should expect to be very familiar with the requirements of GDPR. You will likely understand the flow of data across your organization, have documented the measures you have in place to control and secure it, and addressed any gaps in processes that might see you fall short of the enhanced data requirements that GDPR dictates.

Therefore, the essence of stage three is about managing the newly introduced tools and keeping them up to date. Expect it to encompass:

- Deployment and training on new processes and policies
- Changing existing contracts with third parties and establishing relevant reporting obligations.
- If relevant, empower the Data Protection Officer to drive your GDPR agenda
- A regular audit of the Data Protection Impact Assessments
- A regular evaluation of personal data control effectiveness

Stage 4: Demonstrate Ongoing Compliance

Finally, stage four, and a prediction of how organizations affected by GDPR might be operating beyond May 2018. Clearly, aspects of this may change as the effective date of GDPR approaches, and there is a range of possible outcomes from the previous three stages that might affect the approach you take. However, as possible outcomes exist today, you can expect to focus on the following:

- Internal and external reporting of GDPR efforts (for example, statements surrounding corporate citizenship)
- Publishing of a public privacy notice, as well as a detailed dispute resolution mechanism
- The documented recording of notices and incident handling
- Central storage of all Data Protection Impact Assessments and audit reports
- The possibility of future certification surrounding GDPR compliance and best practice.

Aiming for Business Success

GDPR is non-negotiable, but you cannot forget business success, either. So, while GDPR must be one of your utmost priorities currently, your organization cannot afford to neglect business transformation and growth either.

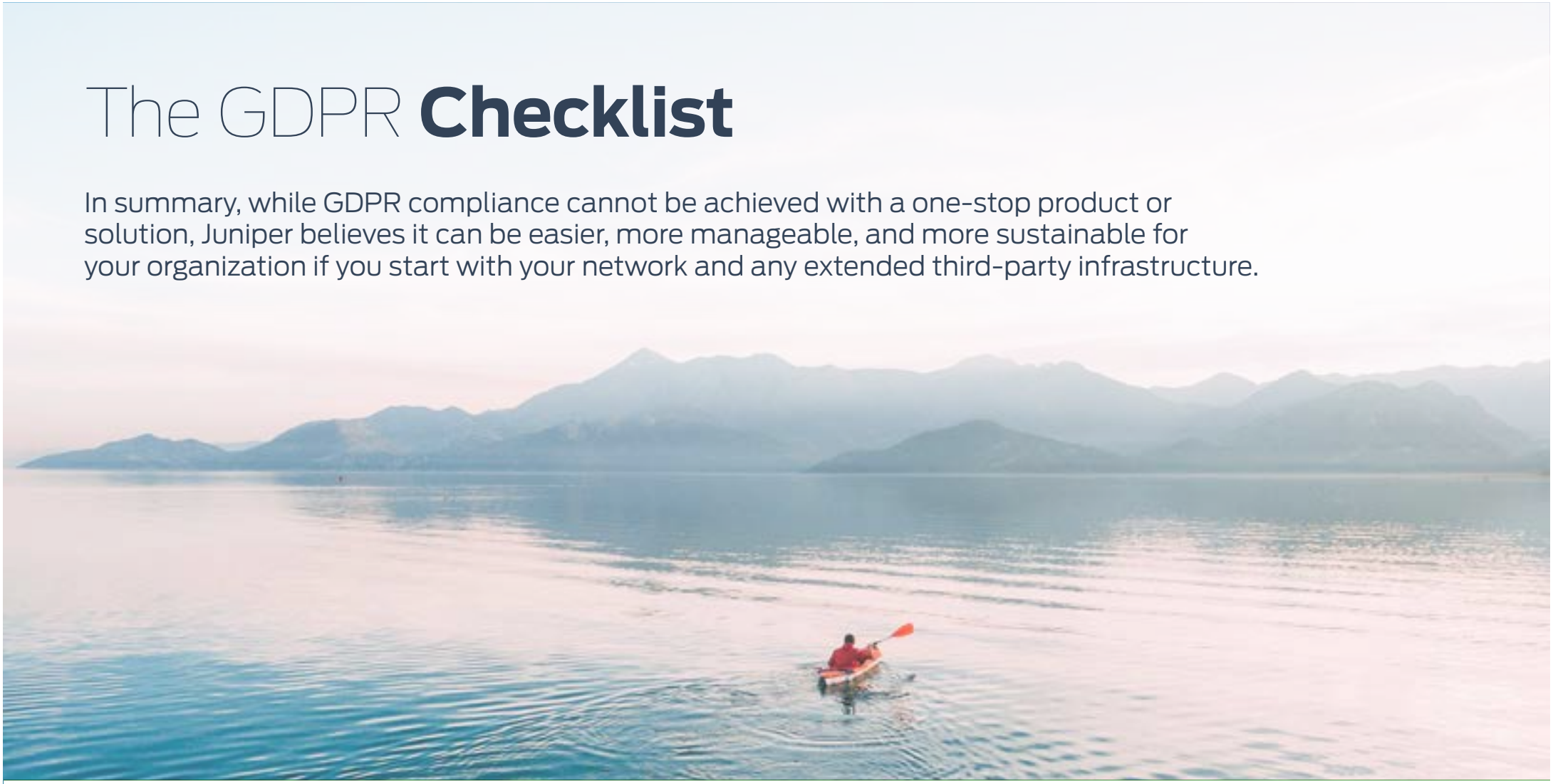
That may sound like a daunting challenge, but actually, there are powerful synergies in starting with your network to achieve either goal. As much as Juniper advocates beginning your GDPR compliance journey with the network – the common denominator platform for all data – we believe that digital transformation and business success start there, too. Whether it is being able to make security a business virtue rather than a reputational headache, turning analytical insights into innovative ideas, or delivering exceptional customer experience online, the right network can be the key.

Juniper Networks helps customers to build intelligent, high-performance secure networks that deliver automation and analytics capabilities as an inherent part of their design. We also strongly believe in the principles of openness and interoperability, enabling you to retain choice and flexibility in your network.

In other words, you can deploy the widest range of best-in-breed solutions for your infrastructure, underpinned by a powerful yet easily deployed and operated secure network. When you are being held to account for your data privacy integrity, and you are relying on digital infrastructure to transform your business, Juniper's unique approach makes a lot of sense on both counts, doesn't it?

The GDPR **Checklist**

In summary, while GDPR compliance cannot be achieved with a one-stop product or solution, Juniper believes it can be easier, more manageable, and more sustainable for your organization if you start with your network and any extended third-party infrastructure.



JUNIPER NETWORKS

BUILD MORE THAN A NETWORK.™

All the data and underlying applications GDPR obliges you to protect and audit use the network. By thinking carefully about understanding the data's security and performance in relation to your network, you are better equipped to develop and enact meaningful policies, deploy effective threat detection and prevention strategies, and provide compliant audit reports.

To finish, here is a checklist of high-priority points for GDPR. Use it to check off the progress you are making towards GDPR. And don't forget, we are on the same journey, so be sure to check in regularly to see how we are solving specific GDPR-related challenges along the way by deploying a range of Juniper solutions. You will find information on the Juniper journey at **juniperemea.net/gdpr**

- ☐ Awareness and understanding of GDPR
- ☐ Discover and understand the information you have
- ☐ Review and update your privacy standards
- ☐ Recognize the rights of the individual in the GDPR
  - Be ready to deal with 'data subject access requests'
  - Outline your legal basis for data processing
  - Update the steps needed to obtain the required consent
  - Implement/modify steps to protect children
- ☐ Implement data-protection-by-design methodology including alerts in case of data protection breaches and an assessment of the notification
- ☐ Set up the right organizational base and empower key stakeholders such as the DPO
- ☐ Think globally when considering GDPR

Corporate and sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888-JUNIPER
(888-586-4737) or
+1.408.745.2000

Fax: +1.408.745.2100

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

Please note:

This eBook contains general information about legal matters. The information is not legal advice, and should not be treated as such.

Any legal information in this eBook is provided "as is" without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information on this eBook.

You must not rely on the information on this eBook as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information on this eBook.

Stay up to date with our GDPR journey and download helpful resources at: juniperemea.net/gdpr

Information correct at time of publication (January 2018).

PN 7400073-001-EN

JUNIPER NETWORKS

BUILD MORE THAN A NETWORK.™