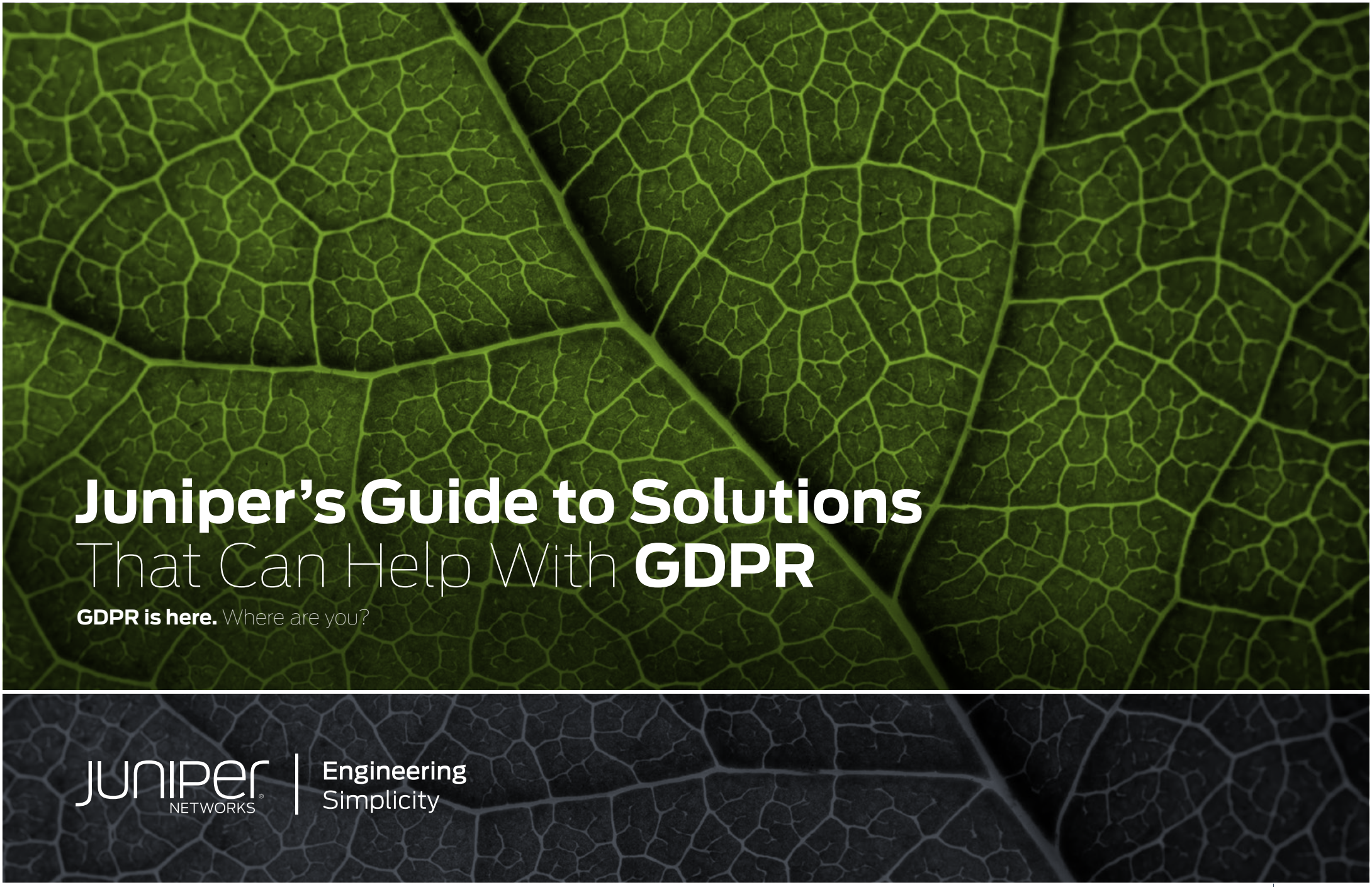


Juniper's Guide to Solutions That Can Help With **GDPR**

GDPR is here. Where are you?

JUNIPER NETWORKS | Engineering Simplicity

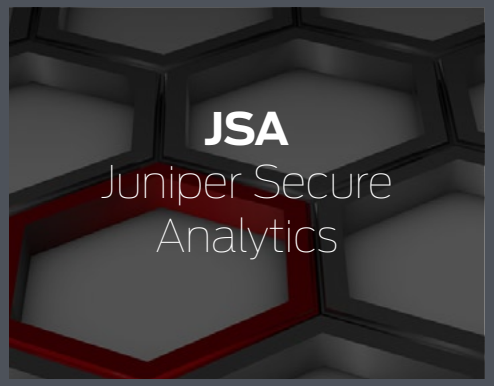
GDPR Solutions

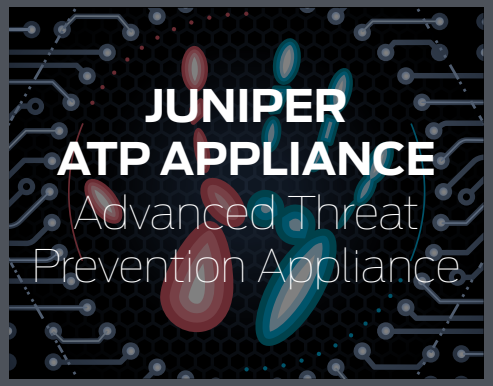
At its heart, the General Data Protection Regulation (GDPR) focuses on the protection of personal data of those located in the EU. Compliance is therefore about your organization's processes, policies and approach to data handling, protection and the surrounding risks throughout its lifecycle, from consent and collection, through usage to storage.

Careful consideration must always be given to data security and performance in relation to your network, simply because every piece of data that your organization manages or uses will touch the network. By doing so, you are better equipped to develop and enact meaningful processes and policies, deploy effective threat detection and prevention strategies, and provide compliant audit reports.

In order to help maintain effective management of your GDPR requirements, we have selected four key solutions from the Juniper Networks portfolio. These deliver an intelligent, automated network that can help you safeguard, analyze and report on data. Any or all of these solutions represent important components that you should consider incorporating into your ongoing, comprehensive GDPR and data privacy/compliance strategy.

Explore our selected solutions below:





Solution 1

Juniper Connected Security

Cyber crime is growing in scale, sophistication and complexity – and it's often taking too long for businesses to react when a breach occurs. A rethink is required; think of the patterns of traffic on your network as your digital fingerprint. Why not make use of that digital fingerprint, analyzing it to generate actionable intelligence which can be shared fast to recognize and reduce the impact of threats?

Under GDPR, once you are aware that a data breach has occurred and that personal data is at risk, you will generally have 72 hours to notify the regulator if you received the data as a "Data Controller" rather than as a "Data Processor" which processes data only at the instruction of a Data Controller (Processors must notify the Controller "without undue delay").

In this window before you have determined that a breach has occurred requiring notification, you will want to focus on understanding what happened, lock down the affected data and begin remediation steps. Having the right tools in place will speed up this analysis. Juniper Connected Security offers you end-to-end visibility and security across your entire network to help with quick identification and mitigation to get business back on track fast.

Solution 1

Juniper Connected Security

Features

- **It's time for a better approach to protecting your organization.** One that keeps you a step ahead of threats. Juniper Connected Security allows organizations to safeguard users, applications, and infrastructure by extending security to all connection points across the network. With Juniper, organizations can achieve more in-depth visibility, in real-time, at the network layer, and build security integrations and automations which protect against both known and unknown threats.
- **Advanced Analytics and Cloud Scale.** You need to identify threats fast, then be able to isolate affected data for analysis. Leverage cloud threat intelligence combined with local network analytics to form a more accurate picture of the scale and impact of a breach.
- **A centralized, global controller/policy engine** that dynamically adapts policy. When security policies are enforced consistently, network security can adapt dynamically to respond to real-time threat information. So, your organization stays ahead of constantly-evolving threats and attacks, even if they are previously unknown.
- **Granular quarantine capabilities** are enabled by different types of security enforcement points in the network, which can include switch and router ports. Even if one application is compromised, you can isolate that threat to protect other critical assets inside.
- **Third-party integration.** Open architecture and a suite of APIs make it simple to choose preferred threat intelligence information sources and remediate across multivendor network infrastructure to give your organization a bespoke, unique security framework.

Benefits

- **Visibility into the network.** Whether the traffic is North-South or East-West, you get full visibility. The entire network becomes a single enforcement domain, and this means that policies can be deployed dynamically, and instantly, to block threats anywhere – not just in firewalls.
- **Comprehensive security.** All firewalls, virtual and physical, are configured with the same policies. This simplifies management and operation and, importantly, ensures consistent security on all devices.
- **Streamlined policy enforcement across the network.** SDSN combines on-site security with cloud-based security services, which provide the foundation for an open policy engine. By providing real-time feedback between firewalls, it makes simple the deployment of policies across network devices the instant they are needed.
- **Rapid and automated threat remediation.** Threats can be identified as they evolve by leveraging threat intelligence from multiple sources (including third-party feeds) and tapping into the power of the cloud.

Learn more about Juniper's Unified Cybersecurity System >>

See Juniper's GDPR Journey >>

Solution 2

Juniper Secure Analytics (JSA)

The GDPR defines best practices for data-governance, meaning you need to understand the data held by your organization and how it is being used. Once you understand the data, spotting any anomalous behavior should become easier – why is that device encrypting its hard drive; why is a laptop exporting data? Individually, these may be harmless actions, but if unexpected they could point to a breach or malware attack.

The integrated approach of JSA, with high levels of data collection, analysis, correlation, and auditing capabilities, enables organizations to quickly and easily implement a corporate-wide security management program that delivers security best practices. These include log analytics with distributed log collection and centralized viewing; threat analytics that deliver real-time surveillance and detection information; and compliance management capabilities – all viewed and managed from a single console.

Solution 2

Juniper Secure Analytics (JSA)

Features

- **All-in-one appliances:** Event collection, flow collection event processing, flow processing, correlation, analysis, and reporting are all embedded within JSA. All core functions are available within the system, ensuring simple deployment and management in minutes.
- **Comprehensive Log Management:** Scalable log analytics are enabled with distributed log collection across an organization, and a centralized view of the information. With storage capabilities ranging from gigabytes to terabytes of data storage, JSA enables long-term collection, archival, search, and reporting of event logs, flow logs and application data that enables logging taxonomy from a centralized view.
- **Threat Analytics:** Advanced network security management solution which bridges the gap between network and security operations to deliver real-time surveillance and detection of complex IT-based threats.
- **Compliance Management:** With 500+ out-of-the-box compliance reports, JSA brings the accountability, transparency, and measurability that are critical factors to the success of any IT security program that is required to meet regulatory mandates. Create, distribute and manage reports that are generated in PDF, HTML, RTF, XML, or XLS formats.

Benefits

- **The ability to reduce OpEx** by collecting all event and flow data in one place with support for a large set of vendors out-of-the-box. Reduce resource management costs with automated updates that download and deploy reputation feeds, parser updates and patches.
- **Rapid deployment capabilities** with preinstalled software, a hardened operating system, and web-based setup: JSA gets your network security up and running quickly and easily. It's designed to provide rapid deployment, fast implementation and improved security, at a low total cost of ownership.
- **The insight to make informed decisions is built in,** with full details on any event and a view of all discovered vulnerabilities, including when they were found and last seen, what scan jobs reported them, and to whom the vulnerability was assigned for remediation or mitigation.
- **Scalable network security management** with the ability to scale to large distributed deployments that can support up to five million events per second. It grows with your organizational requirements.

Learn more about JSA >>

See Juniper's GDPR Journey >>

Solution 3

Juniper Sky Advanced Threat Protection (Sky ATP)

Many data breaches start with an email, or someone clicking on a software link. It can be just that simple and fast. Juniper Sky ATP provides advanced anti-malware and anti-ransomware protection against sophisticated 'zero-day' and unknown threats by monitoring ingress and egress network traffic, and looking for malware and other indicators of compromise. Using multiple technologies in the cloud, Juniper Sky ATP delivers progressive verdicts that assess the risk level of each potential attack and is designed to provide a high degree of accuracy in threat prevention.

Solution 3

Juniper Sky Advanced Threat Protection (Sky ATP)

Features

- **Leverages Juniper's next-generation SRX Series** firewall platforms and cloud-based service components for all management, configuration and reporting. This integration simplifies deployment and enhances the anti-threat capabilities of the firewall.
- **From the cloud or on premises.** Juniper Sky ATP is a cloud-based solution, but if you require an on-premises solution then the Juniper Networks ATP Appliance should be considered, providing protection against a sophisticated and ever-evolving threat landscape.
- **Progressive pipeline analysis engine** starts with a cache lookup against a database of known threats, which is accomplished in near real-time and facilitates inline blocking of malicious content. Malware signatures are added to the cache to ensure immediate identification of recurring threats in the future.
- **Leverages public cloud infrastructure** and encrypted connections on both sides to deliver a flexible and scalable solution. When a threat is identified and blocked, this update is shared instantly into the cloud. This not only expands the breadth and depth of threat intelligence applied to your own infrastructure, but also enables protection for all Juniper Sky ATP customers. So as a Juniper Sky ATP user, you also get the benefits of updates from other users, too.
- **Provides deep inspection and actionable reporting** through comprehensive API support to programmatically deliver dynamic threat intelligence feeds and upload files for analysis, a web-based portal to provision, monitor and manage services, and a rich set of reports and analytics to provide customers with deep visibility into threats and potentially compromised hosts.

Benefits

- **Reduced costs** via automated threat detection and response that is designed to reduce security incidents and improve the productivity and efficiency of security administrators. IT can respond to incidents faster without having to use multiple security tools, saving time and creating savings.
- **Enhanced peace of mind** through a purpose-built system that takes full advantage of modern and innovative machine learning techniques. This enhances the accuracy of threat detection in environments where the volume of alerts often generates false-positives, making it possible for a real threat to get overlooked or ignored.
- **Democratizes IT security** by removing the complexity involved in analyzing and validating security threats. Real-time visibility and protection against previously unseen threats are presented in a way such that you don't need to be a security expert to act.
- **Next-generation security** based on machine learning frees time and allows resources to focus on the big IT and security projects that make a difference to the direction of your organization. With the increased complexity in deploying cloud, big data and IoT solutions, the 24/7 'always-on' nature of cyber crime puts a great strain on IT personnel. Juniper Sky ATP can help to reduce the stress of relentless cyberthreats.

Learn more about Juniper Sky ATP >>

See Juniper's GDPR Journey >>

Solution 4

Juniper Advanced Threat Prevention Appliance (JATP)

The threat landscape is constantly changing, becoming ever more sophisticated and challenging. Protection against today's threats will not be effective against the unknown threats of tomorrow. Couple this with the advent of GDPR and the stringent requirements for breach reporting, and the consequences of a data breach affecting personal data are more severe for enterprises than ever before.

The best way to keep ahead of threats is to establish a security baseline that's defined around 'normal'. If you understand how the network behaves on a normal day, then it's simpler and faster to spot when something abnormal occurs.

The Juniper Networks® Advanced Threat Prevention (ATP) Appliance uses advanced machine learning and behavioral analysis to defend against present and future threats. This combination of technology makes it possible to see when something deviates from the normal security baseline, enabling identification of threats in near real-time. It ingests threat data from multiple security devices, applies analytics to identify advanced malicious traits, and aggregates the events into a single comprehensive timeline view of all the threats on the network.

Fast identification of threats not only reduces the risk of costly damage. It also ensures that the business has as much information as possible to create a remediation plan, which generally needs to be communicated inside 72 hours in accordance with GDPR breach notification requirements.

Solution 4

Juniper Advanced Threat Prevention Appliance (JATP)

Features

- **Open API architecture:** integration with third-party security devices makes for seamless, automatic and comprehensive threat mitigation. This includes quarantining emails on Google and Office 365®, pushing malicious IP addresses to firewalls to block C&C server communications, and isolation of infected hosts through integration with network access control devices.
- **Contextual threat prioritization:** threats are automatically prioritized, calculated from a range of factors such as threat severity, threat progress, asset value and other contextual data.
- **Effective detection techniques:** an advanced suite of techniques including exploit detection, payload analysis, C&C detection, YARA and SNORT rules. These work across a wide range of file types: executables, DLL, Mach-o, Dmg, PDF, Office, Flash, ISO, ELF, RTF, APK, Silverlight, Archive, and JAR.
- **Comprehensive traffic inspection and data correlation:** Traffic across Web, email and lateral spread vectors are inspected, and events are correlated across kill chain stages to monitor threat progress and risk. From this, malware activity is presented in a graphic format and malware traits grouped to help incident response teams better understand malware behavior.

Benefits

- **Gain complete security visibility** through a comprehensive timeline view of a network's threats. Your security team can therefore quickly assess how each attack unfolded with full contextual background information, meaning they can more easily prioritize critical alerts.
- **Respond faster should a breach occur:** time is of the essence when a breach occurs, and if personal data is affected, the GDPR notification is required inside 72 hours. By being able to get full information across every element affected by the threat, you are in a stronger position to demonstrate compliance with GDPR and create an effective remediation plan for your business.
- **Maximize human resource efficiency** with one-touch threat mitigation, which can free up valuable time for your security team to focus on other critical duties.
- **Reduce resource expenditure** with the optional deployment of the ATP Appliance in virtual rather than physical form and minimize the cost of network security refreshes long-term thanks to advanced machine learning that can help detect previously unknown zero-day attacks.
- **Flexible deployment with your existing network infrastructure**, either physically in all-in-one or distributed modes, or virtually in distributed mode only.

Learn more about JATP >>

See Juniper's GDPR Journey >>

Conclusion

The GDPR requires thorough, comprehensive and accountable protection of personal data and defines best practices for data governance. Cybersecurity is a core component of successful GDPR compliance, to analyze, protect and mitigate. The right security solutions will not only work to keep malware and threats outside of your network - they will also use security analytics to ensure that you are in the best possible position to understand quickly what was affected, what happened, and how to get business back on track fast if a breach does occur.

For more information on Juniper solutions and GDPR visit our web-page:

Juniper GDPR solutions >>

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

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

PN 7400074-002-EN

Juniper Networks | Engineering Simplicity

Please Note:

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

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

You must not rely on the information in this guide 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 in this guide.

Information correct at time of publication (April 2020).