In May of 2018, the European Union put the General Data Protection Regulation (GDPR) into law - a landmark piece of legislation across the entire Union that would enforce accountability regarding privacy and data protection for all entities that process personal data of European Union persons, whether located in the Union or not. This legislation builds off of long decided and agreed upon rights to privacy for European Union citizens, specifically in the 1950 European Convention on Human Rights that stated that “everyone has the right to respect for his private and family life, his home and his correspondence.” From this basis and beyond, the GDPR has been the guiding force towards protection of data and online privacy amongst Union citizens, but due to the extension of Virtual Private Networks across the world, other nations’ citizens can benefit from this legislation to certain extents of its implementation.

Virtual Private Networks (or VPN’s, as they are most commonly known) are a crafty means by which an end user can tunnel their own personal connection through another one by behaving as if it were locally connecting to such. In doing so, a user can tunnel a public network through a privately hosted one that will encrypt outgoing data and, therefore, provide secure web traffic for the user in comparison to the open connection they would initially have utilized. However, a caveat arises in this seemingly perfect method of securing internet safety, which is that VPN’s must legally keep logs of connections and browsing contents. This contradicts the entire purpose of the security and privacy innate to the usage of VPN’s, as these logs would be required to be presented to authorities if requested accordingly or face penalties, including but not limited to the removal of VPN licensure.

With the introduction of GDPR, however, European Union based VPN’s have experienced a revival and return to form. As per GDPR’s official statutes, no Union VPN provider will be allowed to keep browsing logs as doing so would be a criminal offence, as this would constitute holding personal data without consent. In a similar manner, while connection logs can still be kept by VPN providers, any user can request to have these logs deleted under GDPR and the provider must oblige so as to avoid criminal offences here as well. As a result of these guidelines and their enforcement on all European VPN companies, as well as any VPN’s that have servers based in EU territories, VPN’s based in the European Union have become much more focused and are back to exhibiting their image as secure, private, remote connections for users.

Unfortunately, these guidelines only protect European Union citizens and entities based within such. However, the usage of VPN’s with servers based in the European Union is a clever means by which international citizens can benefit from the statutes present within GDPR. By connecting to one of such VPN’s, citizens from outside the European Union experience the same treatment as users from the European Union would as the VPN provider itself must treat all incoming users the same by only recording connection logs. Similarly, many VPN services based outside of the European Union are adjusting their privacy policies in order to be compliant with GDPR, so as to both be usable within the Union and to instill confidence in users across the globe.

Despite the lack of similar legislation outside of European Union territories, the GDPR’s functionality and effect upon the data retention of VPN providers within their jurisdiction has provided a unique opportunity for international citizens to benefit from these statutes. Going forward, many companies and governing bodies likely will, and many have, begun altering their policies and legislation to be more in line with GDPR, with the most relevant of such being the passing of the California Consumer Privacy Act that echoes many of the beats that GDPR lays the groundwork for. For now, however, American and other international citizens must do what they can with their current privacy rights and those second-handedly afforded them by usage of European based VPN’s.

**Works Cited**

Baig, Anas. “Why Do VPNs Need To Be GDPR Compliant?” *Infosecurity Magazine*, 6 July 2018, www.infosecurity-magazine.com/opinions/vpns-gdpr-compliant/.

“Does the GDPR Apply to Your US-Based Company?” *Workplace Privacy, Data Management & Security Report*, 10 Jan. 2018, www.workplaceprivacyreport.com/2018/01/articles/international-2/does-the-gdpr-apply-to-your-us-based-company/.

“General Data Protection Regulation (GDPR) Compliance Guidelines.” *GDPR.eu*, gdpr.eu.

Weisman, Steve. “How Does a VPN Work?” *NortonLifeLock*, us.norton.com/internetsecurity-wifi-how-does-a-vpn-work.html.

“What GDPR Means for VPN Providers (and Users).” *GlobalSign GMO Internet, Inc.*, 7 Feb. 2020, www.globalsign.com/en/blog/what-gdpr-means-for-vpn-providers-and-users.

“What Is GDPR and What Do VPNs Have to Do with It?” *VPNPros*, 25 May 2018, vpnpros.com/blog/what-is-gdpr-and-what-do-vpns-have-to-do-with-it/.