BEYOND THE BASICS

Personal risk management tips provided by: Crendon Insurance Brokers Ltd

Did You Know?

Fallout from the Facebook Cambridge Analytica scandal and expanded user rights from the GDPR now empower you to force social media giants to delete your old, embarrassing posts. In March 2018, Facebook confirmed that a third-party app had unlawfully harvested data relating to nearly 87 million people across the globe, including 1 million UK citizens, which was then shared with an organisation called Cambridge Analytica. In the midst of recurring data breaches and expanded control over your data under the GDPR, rely on these tips to increase your social media data privacy.

CONTROLLING YOUR SOCIAL MEDIA DATA

Why is my data being collected?

Political campaigns, social media companies and commercial organisations collect your personal data for a variety of reasons. However, the most common reason is for microtargeting.

The ICO defines microtargeting as a form of online-targeted advertising that analyses an individual's personal data to further understand the interests of a specific audience or internet user. By collecting this data, an organisation is able to influence an individual's actions with personalised messages and advertisements.

You may be exposed to microtargeting online either via social media providers or third parties operating on social media. To confirm whether this is the case and to strengthen your privacy settings on each platform, click the links below.

- Facebook
- LinkedIn
- Instagram
- Twitter

How can I protect my data?

When it comes to protecting your personal data on social media, each social media provider has a different set of tools to help you do so. Generally, each provider should allow you to view data collection settings under specific tabs within your account, such as 'account settings' or 'privacy preferences'. These settings will allow you to tailor your information for more personalised advertisements, as well as limit microtargeting practices altogether.

In addition, it is important to always pay attention to what personal data you share on social media through posts and interactions, the provider's privacy policy and how the social media service is using your data.

Lastly, remember that even if you delete an app from your phone, it doesn't necessarily delete the personal data it collected. Be sure to contact the app supplier to understand how your data will be used after deletion.

The Right to Be Forgotten

As part of the GDPR requirements, you also have the ability to extend your 'right to be forgotten' within the realm of data collection and processing. UK consumers have the right to request that their personal data be erased after a certain period of time. The purpose of this guideline is to allow for long-time social media users to delete outdated or embarrassing content from their profiles, such as old Facebook posts.

For more information on controlling your social media data, visit the ICO's website, or click the provider-specific links above.

Crendon Insurance Brokers Ltd
www.crendoninsurance.co.uk
0121 454 5100

Crendon Insurance Brokers