HTA guide for members using WhatsApp groups

Introduction

The HTA operates a number of WhatsApp groups (referred to in this guide as **Groups**) which enable members to communicate with one another. We are aware that some members are using these Groups to share personal data, in particular when following the recommendations of their local police forces to share crime information with other members.

This short guide is designed to help you navigate the data protection issues arising from using the Groups in this way. It is not a substitute for legal advice and if you have any concerns about what personal data you are lawfully able use and share, you should seek advice before doing so.

There is a wealth of information available on the website of the Information Commissioner's Office (**ICO**) at: https://ico.org.uk/for-organisations/.

SME members may find the ICO's small business advice hub particularly useful: https://ico.org.uk/for-organisations/advice-for-small-organisations/

What is personal data?

Personal data means any information which identifies a living individual. You probably have personal data about your customers and others, for example, names, addresses, emails, telephone numbers, debit/credit card details, photographs, videos and CCTV footage. It can also include more sensitive information, such as details about a person's health or their criminal record.

Why does data protection matter?

We live in a data-driven world and if you use personal data in your business, it is important to follow the rules.

The ICO can fine businesses which don't comply with the rules and doing the right thing should also help to protect your reputation and maintain your customers' trust.

Basic principles

In the UK the protection of personal data is governed primarily by the UK General Data Protection Regulation (**GDPR**). It is designed to ensure everyone's data is used properly and fairly, and not used in ways people wouldn't expect.

The GDPR sets out seven key principles which, simply put, provide that:

1. Personal data must be processed lawfully, fairly and in a transparent manner.

2. It must be collected for specified, explicit and legitimate purposes and used only for those purposes.
3. It must be limited to what is necessary.
4. It must be kept up to date and inaccuracies should be corrected.
5. It should be retained for no longer than is necessary.
6. It should be stored using appropriate security to protect against unlawful use and against accidental loss and damage.
7. The data controller (the person collecting/using/sharing the information) must be able to demonstrate compliance with principles 1-6 above.

The principles aren’t hard and fast rules, but they capture the spirit of the data protection regime, and you should use them to guide the decisions you make.

Sharing personal data via the Groups

Sharing data can be a good thing but it’s important that you understand how to share data lawfully, fairly and transparently and take all the necessary steps to keep it safe.

We recommend that you consider the following matters before sharing personal data via the Groups (and also before using the personal data you receive from other members of the Groups):

A. What information are you holding and do really need to use/share all of it? Don’t keep anything ‘just in case’.

B. What is your ‘lawful basis’ (in other words your valid reason) for holding and sharing the information? Please see below for more about this. Remember to keep a record of your decision.

C. How will you keep the information secure while it is in your possession?

D. Make sure you explain (for example in the privacy policy on your website) that you may use and share this data with other members for the purpose of helping to prevent and detect crime. Remember to periodically review your privacy policy and keep it up to date.

E. Remember to delete the information when you no longer need it.

What is your lawful basis for using and sharing personal data via the Groups?

The GDPR sets out various ‘lawful bases’ (valid reasons) for using personal data.

Consent is sometimes a ‘lawful basis’ for using personal data but in the context of sharing information about known or suspected criminal activity, consent won’t be appropriate. Instead, your lawful basis is likely to be one of the following:

- Legal obligation: you need to use and share someone’s information because you have to by law. For example, you may need to share information with the police if they have a warrant for information you hold about someone.

- Legitimate interest: the use of the information is necessary to fulfil a specific and reasonable (‘legitimate’) interest of your business. You need to weigh up (a) the interest to your business of using and sharing the information versus (b) the interests of the suspect in keeping this information private.

As the ICO website explains *“A shopkeeper can share CCTV footage with the police if there’s a court order or if it’s relevant to a police investigation - and in this situation, the shopkeeper wouldn’t need to inform the suspect. Sharing this type of information is justified, despite the potential impact on the person who it’s about, because of the need to protect us all from criminal activity”.*

A similar approach could apply when sharing information with HTA members via the Groups but take into account all relevant matters, such as:

- Have the police asked you to share the information, and does their request seem reasonable?
- What information really needs to be shared? For example, it may not be relevant to share with others information (if you have it) about the suspect’s sexual preference, ethnicity, medical condition or political views.
- Does the information need to be shared with all members of the Group or would it be better to direct message just some members, e.g. those most local to you?