Transcript: Data Protection During Christmastime podcast – What you need to know

Hello and welcome to the Data Protection Commission Podcast with me Graham Doyle Deputy Commissioner and Head of Media Communications here at the DPC.

As you approach Christmas time and the busy shopping season we thought it might be helpful to give you a run through some of the DPC's guidance around issues that crop up the most at this time of year. So in today's podcast we're gonna look at topics of connected toys and devices, e-receipts and direct marketing. If there's a particular topic that you're interested in learning more about you can find links to our guidance on our website which is at www.dataprotection.ie.

Firstly I'm going to delve into some advice on the different connected toys and devices which may be gifted, particularly to children at this time of the year. Many adults and children derive lots of utility from the connected toys and devices that are on the markets today. The purpose of what I want to discuss now is just to raise some awareness of some of the data protection concerns and issues that we do need to be aware of as we're using or allowing our children to use these devices.

As people would be aware, connected toys have the ability to interact with children either directly or through an accompanying app, in some instances the toys can recognize words and react in certain ways to suggest an emotional response of some sort to what a child says or does. A lot of people would be familiar with dolls that close their eyes when asked to go to sleep by the child. In some cases these toys connect to an app and it might allow for the collection recording of conversations between a doll and a child or even act as some form of walkie-talkie. It's important to know that for some of these products the voice recordings are shared with other companies and the toys terms and conditions may allow for the child's conversation to be used as a basis for targeted advertising.

Certain toys may also be advertised as using AI to appeal to some children. This could mean that more data will be collected and that it will be subject to complex process which may result in a profile being created about a child. Smartwatches are another common gift both for adults and children. Similarly

these can allow parents or guardians to communicate with their child through a mobile phone function and or parents can check the location of a child. These things can be very useful. Many may also feature a quick dial capability if there's an emergency, but it is important to note that in some cases these communications functions are not secured and can be hacked. This would allow eavesdropping on conversations or even serious issues such as direct communication with the child themselves. The location functionality in watches can also be manipulated at times by hackers to make the child appear somewhere else and the SOS function can even be tricked to use a non-trusted phone number. So any interaction that your child may have with these toys smartwatches or other similar smart devices can potentially carry some data protection risk.

Whilst many of us use these products as part of our daily life, it's important that we are aware of these risks. In our guidance notes we have a full list of things to look out for in this area and we do encourage parents and guardians or anyone who wishes to give the child with a similar device, to give careful consideration when selecting one that has a camera or some sort of voice starting ability that connects to the Internet, or that allows remote connection using a smartphone or tablet app.

If you are happy with the device, take care to ensure that it is working in the way described and that you are happy with what it's doing, especially when it shares information with an app or with companies websites.

Moving onto e-receipts. This is another topic which is particularly relevant as this time of the year with an increasing number of retailers at point of purchase offering customers the option of receiving an electronic receipt or an e-receipt as it's commonly known.

The DPC previously carried out a series of audits in order to assess how organization process personal data in the course of providing e-receipts to customers. In a number of cases e-mail addresses gathered for the purpose of issuing you receipts were then subsequently used by retailers in order to issue marketing materials. Following on from these audits the DPC produced guidance around the use of e-receipts to assist retailers to adhering to the best practice. It's important that customers know their rights in this regard. At the point of purchase if a customer is asked to provide an e-mail address they should be advised if the reason is to provide them with an e-receipt and it should be made

clear that they are under no obligation to provide this e-mail address in order to get that receipt. They can always request a hard copy from the till.

If an e-mail address has been collected for the purpose of sending an e-receipt and the retailer then wants to use that address for sending marketing emails, we always advise that unless the retailer has informed the customer about this and has given the customer the opportunity to opt out of receiving these marketing emails at the point of collection, then it is unlawful for the retailer to do so. The customer should always have an easy opportunity to opt out afford to them each time they are subsequently contacted for marketing purposes. Data Protection law requires retailers to process data transparently and also to be accountable to both the customer, whose data they process, and towards us here at the DPC. Retailers who want the send marketing emails in this way must comply with the rules as they are stated in both the GDPR and the e- privacy regulations. Both of which also go in our next topic of discussion which is electronic direct marketing.

Electronic direct marketing usually involves an organization or a marketer attempting to promote a product or service, or attempting to get you to request additional information about a product or service, by targeting an individual. The DPC tends to receive lots of queries on these types of communications and people regularly asking how can I opt out from using them. Typically such marketing communications sent by e-mail, text message, or by way of telephone calls, again commonly known as cold calling. The communications often contain special offers or promotions but direct marketing can be broader than sales pitches as it can also include canvassing for votes in an election or the promotion of the ethos of an organization. If you receive electronic direct marketing when you have not provided your information to an organization or if you did not provide it for the purposes of the marketing this is known as unsolicited direct marketing. You may or may not have directly provided your contact information to an organization but nevertheless this does not always mean you provided your contact details in order for an organization to market their products or services to you.

You can stop an organization sending further unsolicited direct marketing to you by sending an unsubscribe or opt out request to the organization that sent you the marketing material in the 1st place. The material you receive should always

include a valid address to which you may send to. Your unsubscribe request must be actioned.

Most of us of are probably familiar with seeing these and emails marketing emails that we receive, however it's important to note that not all marketing communications sent by an organization involved the processing of personal data and therefore data protection regulations do not apply in those situations. For example a market survey seeking your views on issues such as political matters or radio listenership preference. But if have received direct marketing from an organization you never dealt with before and if you have concerns as to where your information was sourced, you can seek and should seek an explanation from the organization concerned.

Where you're unhappy with the outcome of this you can of course come to us here at the DPC for further advice. Infringements of the rules governing unsolicited direct marketing is a serious matter as such infringements are treated as criminal offences which may be prosecuted by the DPC in the District Court, where penalties of up to €5000 may be imposed for each offense. We regularly see prosecutions of this nature taken before the courts. if you're see marketing that break the rules, you may submit your concern to the DPC outlining the details to our online form on our website. You can also find a host of guides on this topic on our website.

We're all wrapped up with today’s DPC podcast. I'd like to thank you for joining me hopefully you learned something useful as we approached this festive season. This is really about awareness raising for individuals, customers, organizations and retailers themselves. I'd like to wish you and your families a happy and safe Christmas period and we will be back in the New Year with our next podcast episodes.

Thank you very much for listening.