Guidance on Connected Toys and Devices

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Many children enjoy playing with toys and devices that have the ability to interact with them, either directly or through an online 'app'. The popularity of these toys and devices, which can provide a fun and educational experience, along with advances in technology, means that there are more and more of these products on the market to choose from. With this in mind, the Data Protection Commission (DPC) has put together this short guidance to assist you if/when you decide to purchase one.

Toys and Devices

Connected toys, in particular dolls, may give the appearance of having a personality and human-like quality to appeal to children. In some instances, the toys can **recognise words** and **react** in certain ways to suggest an emotional response to what the child says or does.

Some toys also **connect to apps on smartphones or tablets**, which might allow for the collection and **recording of "conversations"** between the doll and the child, or even act as a **walkie-talkie**. 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 conversations to be used as the basis for **targeted advertising**. Toys may be advertised or promoted as using "artificial intelligence" to appeal to certain children. Generally this means **more data will be collected** and that it will be subject to complex processing which may result in a profile being created about your child.

Smart Watches

Similarly, smart watches **can allow parents/guardians to communicate** with their child through a mobile phone function, and **report the location** of the child. Some watches feature an "SOS" button to allow a quick dial capability if there is an emergency. However, it has been found that in **some cases** the communications functions are **not secure and can be hacked** allowing eavesdropping on conversations, or even direct communication with the child. The location function can also be manipulated by hackers to make the child appear somewhere else, and the "SOS" function can be tricked to use a non-trusted phone number.

Legislation

Under data protection legislation, if your child is under 16, a manufacturer of such toys or "data controller" collecting and processing personal data, **where they are relying on 'consent'** as the legal basis for processing, is required to obtain **parental/guardian authorisation** to process it. How this happens may take various forms, but

parents/guardians should ensure that they are asked for authorisation, that they understand who the data controller is, why the personal data is being collected and how it is secured. In addition, parents/guardians should be able to exercise their right to **withdraw their consent**, to find out or access the personal data that is retained, and/or how to have it deleted.

Any interaction your child might have with these toys, smart watches, or other similar smart devices is a potentially sensitive matter. Parents/guardians who are considering buying them this Christmas may wish to **take extra care** when selecting one that has a camera or voice-recording ability, connects to the internet, allows remote connection using a smartphone or tablet app, or has a location tracking facility.

What to Look Out For

- ✓ Can you **easily understand** the terms and conditions and the privacy/data protection implications of the child's use of the toy/device?
- ✓ Where the controller has asked for **consent or authorisation** for processing, are you given the opportunity to consent to each purpose and to control the use of your child's personal data?
- ✓ Are you **asked to authorise** the processing of your child's personal data – their voice or location, for example? Where the controller has asked for consent or authorisation for processing, is it **clear how you can withdraw consent** or authorisation for the processing of your child's data?
- ✓ Has the controller given you in**formation on how to exercise your data protection rights**?
- ✓ What kind of "**sensors**" does the toy/device have – for example, would it record your child's voice? Can it understand certain words or phrases? Can it take photographs or allow video to be captured?
- ✓ Does it have a **GPS** or other means to track **location**?
- ✓ Can the toy/device connect to the **internet** or use **Bluetooth** to connect to an app that you install on your smartphone or tablet?
- ✓ If there is an **app** that you can use with the toy or device, can anyone download and use it or just kids (or parents/guardians) who have the device?
- ✓ Does a button on the toy/device have to be used, or does the toy have to be used in a certain way in order for the app to connect to it?
- ✓ Can you **turn** the other **sensors**, network **connection**, or location **tracking on and off**, or does the child have to press a button each time in order for them to work?
- ✓ **Is it clear** to the child and to you **when the sensors are working** – for example, do the toys or devices light up or make a noise when the sensors are activated?
- ✓ Is it **clear on the packaging or manual** that comes with the toy/device how the sensors work and what you can do to control them?

- ✓ Does the **packaging or instructions make it clear** if the information collected is also **sent across the internet** to the manufacturer or any other companies or websites?
- ✓ Does the packaging or instructions say that the information is collected "**securely**", using terms like "*https*" or "*ssl*" or "*tls*"?
- ✓ Where information is shared with others, are there **contact details** for these organisations? Do the companies' websites have **privacy policies** that allow you understand what they do with the information they collect, how long they keep it for, and allow you to get in touch and ask that the information be erased?
- ✓ If you have to **register on a website** to open an account for the toy or an associated app, does it give you a "dashboard" or "portal" to see what information is collected and allow you to control it? (Specifically, can you request that personal data be deleted, stop it being collected, or stop it being used for things like advertising/third party sharing?)

If you find that the answers to these questions cannot be found or that you are not happy with them, then our advice to you is to **give careful consideration** to purchasing the toy/device. If you are happy to buy the toy/device for a child, then take care to ensure that it is working in the way described, and that you are happy with what it is doing, especially when it shares information with an app or with companies or websites it might connect to.

Note:

In 2016, the **European Consumer Council** contacted Data Protection Authorities around Europe to **raise concerns** regarding possible data protection issues that might occur when children and parents/guardians use **toys with microphones and cameras** that have an ability to connect to the internet. In October 2017, a similar notification was issued by the European Consumer Council regarding **smart watches** aimed at the children's market.