THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL

Internet of Things (IoT)

Risk Manager Checklist, Europe

Salen Churi, Assistant Clinical Professor of Law
Bluhm-Helfand Director of the Innovation Clinic
The University of Chicago Law School

Harrison Hawkes, Student
The University of Chicago Law School Innovation Clinic

Research made possible
through a generous grant from

AIG

RISK + INNOVATION I PART 5 IN A SERIES
www.aig.com/innovativetech

What's Inside

Acknowledgements

The Innovation Clinic at The University of Chicago Law School and AIG would like to thank the following, among others, for their contributions and insight during the creation of the checklist:

Naresh Shah, VP of Shared Services at A^3 by Airbus; **Jay Parmar**, Director of Policy and Membership at BVRLA; **Maciej Kranz**, VP of Corporate Strategic Innovation at Cisco; **Jonty Roberts**, Insurance Industry Advisor in the Digital Transformation Group at Cisco; **Roxanne Morison**, Senior Policy Adviser - Digital at CBI (Confederation of British Industry); **Amanda McCallion**, Risk & Insurance Manager at CRH Plc; **Giulio Coraggio**, Partner, Global Co-Chair of the Internet of Things group at DLA Piper; **Martin Strutt**, Region Director at EEF; **Arnaud Constanty**, Risk & Insurance Management at Europcar International; **Gareth Eggle**, Head of Insurance at Flint Hyde London Ltd; **Alexander Bauer**, Business Development Executive, Leader of Insurance at IoT Industry Lab at IBM Watson IoT HQ; **Christian Bieck**, Insurance Practice Leader, IBM Institute for Business Value; **Jürgen Huschens**, Industry Technical Leader & CTO Insurance at IBM Europe; **Anders Søborg**, Head of Risk Management, VP, Group Risk Management at ISS World Services A/S; **Joe Policella**, Business Consulting Managing Principal at NTT DATA Services LLC; **Cinthia Granados Motley**, Partner at Sedgwick LLP; **Sofia Trope**, IoT Business Developer at Telenor; **Hans Graux**, Founding Partner at time.lex; **George de Boer**, Leader of Connected Car Initiatives at TomTom.

We would also like to thank **Dr. Mechthild Rohen**, Head of Unit 'Internet of Things' in DG CONNECT, and **Nikolaos Isaris**, Deputy Head of Unit 'Internet of Things' in DG CONNECT, at the European Commission for speaking with us on the European Commission's efforts regarding the IoT.

Lastly, we are grateful to **Norton Rose Fulbright** for sharing their insight and experience in the preparation of this checklist. However, Norton Rose Fulbright does not in any way endorse the contents of this checklist and does not in any way accept liability or any form of duty or responsibility for those contents.

Definitions

The overall goal of the checklist is to ask the right questions in order to help risk managers and other readers identify and assess risks associated with their IoT technology. The checklist is not legal advice. Rather, it is designed to allow readers to perform much of the legwork on their own in mitigating or eliminating IoT-related strategic and legal risks.

Please note that readers should consider both B2B and B2C concerns while reading the checklist.

The following terms are used throughout the checklist. Please note that some of the definitions below are unique to the checklist and do not necessarily apply outside of the checklist.

Anonymise: Data that are anonymised cannot be attributed to a data subject. Fully anonymised personal data falls outside the application of the GDPR

B2B: A business-to-business relationship/transaction

B2C: A business-to-consumer relationship/transaction

Bystander: A third party who is not using the IoT technology

Data Subject: A natural person from whom personal data have been collected

Interoperability: The ability for an IoT technology to communicate or exchange data with another IoT technology

IoT Technology: All IoT devices and systems

Personal Data: Any information relating to a natural person who can be identified

Pseudonymise: Data that are pseudonymised can still be attributed to a data subject by the use of additional information

User: Person or entity that uses the IoT technology

Introduction

Salen Churi
Assistant Clinical Professor of Law
Bluhm-Helfand Director of the Innovation Clinic
The University of Chicago Law School

With the growth of the Internet of Things (IoT), the lines between the worlds of atoms and bits, between hardware and software, are blurring. As physical sensors, feeding data into machine learning-enabled digital platforms, have become ubiquitous, the digital world is increasingly superimposed on the physical world. As a result, this digital layer that sits atop the physical world is injecting new risks into old areas of life and shifting liability in profound ways. Two years ago, AIG and the Innovation Clinic at the University of Chicago partnered to shed light on this emerging category of risk, creating a practical guide for risk managers as they are relied upon to help define and forecast exposure in this new world.

Last year, we released the IoT Risk Manager Checklist, where we addressed the challenges that faced companies operating in the U.S. who wished to implement IoT into their products and services. The overwhelmingly positive response highlighted to us that we were on to something. Many readers shared that they operated internationally, and that operating in European markets posed significant and unique challenges, so it would be helpful to apply our approach to Europe. In particular, because IoT deals principally with data, the looming implementation of the EU's General Data Protection Regulation (GDPR) made it even more critical to offer guidance on how this would affect IoT products and services. So we set out to build on the insights we had gleaned from the original U.S. version of the IoT Risk Manager Checklist and apply them to the unique challenges facing companies operating in European jurisdictions in 2018 and beyond.

As with the original Checklist, we needed a partner with the broad reach to bring in partners who could help us learn about best practices across different industries, but also the depth and thought leadership to help us sharpen our thinking and focus our research. As a leading insurance company and innovation thought leader, AIG was an ideal partner in crafting this checklist. Their support was invaluable in granting us access to perspective from leaders who are on the front lines of these new innovations across multiple industries and different types of products, services, and business processes. We are grateful to all who are in the acknowledgements.

On May 25, 2018, the GDPR will come into effect in the EU. This checklist aims to focus risk managers on the aspects of GDPR, among other influences, that will affect IoT products and processes in advance of this critical milestone. I hope this document will enable risk managers to better balance risk with reward of integrating IoT-related enhancements into products, services, operations and overall governance models. As with any cutting-edge legal or regulatory environment, there are no easy answers. This checklist is meant to help the risk managers ask the right questions as IoT becomes increasingly pervasive in their businesses.

Human vs. Machine Error Examples and Considerations

I. Autonomous Vehicles

A driver is driving an autonomous vehicle (AV) that is in autonomous mode. The AV crashes into an oncoming lorry as the latter turned and crossed the road's median and into the AV's path. At the time of the accident, the AV is in autonomous mode and the driver does not have his hands on the steering wheel despite being contractually obligated to do so, even when the vehicle is in autonomous mode. Both drivers are injured and both vehicles receive substantial damage. Assume that the lorry made a proper turn and that all fault rests with the AV and its driver.

Issues to consider:

a. What procedures are taken to determine whether the AV's driver, AV manufacturer, autonomous system creator, or any other party is liable?
   i. See: Product Liability I

b. How is the liability assigned?
   i. See: Liability Assignment Amongst Multiple Parties III

c. What testing was previously completed?
   i. See: Product Liability IV, VI

d. What continuous testing and maintenance are completed, especially after the accident?
   i. See: Product Liability V, VII

e. Was the driver properly informed of the risks of driving an autonomous vehicle?
   i. See: Product Liability II, III, VIII, IX

f. How enforceable is the driver's contractual obligation to keep his hands on the steering wheel when the AV is in autonomous mode?
   i. See: Contract and Tort Liability I

II. Home Automation

Your company sells an IoT thermostat that allows users to adjust the temperature of their homes from their mobile devices. The thermostat is perpetually collecting data and sending them to your company, including the temperature in a user's home. One day, the thermostat registers a dramatic spike in the room temperature due to a fire. Your thermostat is not a smoke detector.

Issues to consider:

a. Has your company incurred a duty to warn the IoT thermostat's user of the fire despite not being a smoke detector?
   i. See: Contract and Tort Liability I; Product Liability VIII

b. If your company has incurred a duty to warn, how do you give reasonable and timely notice?
   i. See: Contract and Tort Liability I; Product Liability VIII

c. If your company has incurred a duty to warn, can your company contract out of such a duty or is it inherent and unavoidable?
   i. See: Contract and Tort Liability I; Product Liability II

d. What do your IoT thermostat's terms of use state are the capabilities of your IoT thermostat and are users aware that it is not a smoke detector?
   i. See: Contract and Tort Liability I; Product Liability III, IX

e. Has the user of your IoT thermostat incurred any duties towards bystanders?
   i. See: Product Liability III, IX, X

III. Industrial Control Systems

A malicious third party hacks into your company's ICS and takes control of a robotic arm on an assembly line. The third party causes the robotic arm to swing erratically. The employee responsible for controlling the arm fails to enact safety protocols in order to properly shut down the arm, and the erratic robotic arm severely injures another employee.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
   i. See: Cybersecurity II, III, IV

b. How is liability assigned between the company, the negligent employee, and the malicious third party?
   i. See: Liability Assignment Amongst Multiple Parties III

c. Was this a foreseeable risk? If yes, why was it not prevented?
   i. See: Cybersecurity II, III, IV; Product Liability II, III, IV, VI, VII

d. Have any peer organisations suffered similar breaches?
   i. See: Cybersecurity III

e. Was the injured employee aware of such a risk and given the opportunity to opt into such a risk?
   i. See: Product Liability VIII, IX, X

IV. Pharmaceuticals and Healthcare Devices

Your company manufactures and sells IoT pacemakers. The CEO of a public company secretly has pacemaker surgery that uses one of your pacemakers. A malicious third party hacks into the pacemaker to retrieve personal data on the CEO's health, which is poor, and releases these data to the public. The company's stock price subsequently falls, costing investors millions of dollars.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
   i. See: Cybersecurity II, III, IV

b. How liable is your company for both the release of the CEO's personal data and the drop in stock price, especially if the CEO and her company knew the pacemaker was an IoT technology?
   i. See: Cybersecurity III; General Data Protection Regulation (GDPR) III, XI, XIV, XV; Liability Assignment Amongst Multiple Parties II, III

V. Smart City

In a major metropolitan area, a malicious third party hacks into a commuter train's system owned by your company and causes the train to crash into the next station at an accelerated speed, causing many injuries and property damage. It is later determined that the breach would not have occurred had the train's system been properly updated.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
   - i. See: Cybersecurity II, III, IV

b. Who is liable for steps not being taken to properly update the train's system?
   - i. See: Cybersecurity II; Liability Assignment Amongst Multiple Parties III; Product Liability V

c. When is the train system tested and updated?
   - i. See: Product Liability V, VI, VII

d. Did the commuters know that the train on which they were riding was an IoT technology? Did your company incur a duty to warn the commuters?
   - i. See: Product Liability III, VIII

e. What duties of care did your company's IoT technology, the train, cause you to incur in regard to the commuters?
   - i. See: Product Liability III, IX

VI. Unmanned Aerial Vehicles (a.k.a. UAV or drones)

Your company's drone flies near a fire in a business park while delivering a package to a customer's office. The presence of the drone prevents firefighting helicopters from successfully extinguishing the fire. The fire subsequently spreads to other office buildings, resulting in millions of dollars in damage.

Issues to consider:

a. What further damage was caused due to your company's drone presence and how is liability assigned for the additional property damage?
   - i. See: Liability Assignment Amongst Multiple Parties III

b. What legal considerations exist surrounding the operation of a drone, especially around first responders and their vehicles/equipment?
   - i. See: Product Liability I

c. How does your company prevent another similar incident from occurring?
   - i. See: Product Liability II, IX, X

The IoT Checklist

Strategic Considerations

I. General

1. What incentives do users of our IoT technology have for giving consent to the collection of their personal data? How do those incentives change based on whether users are individuals or businesses?[1]
   a. Are users given a price discount or additional services for providing consent?
2. What happens if users refuse to consent to the collection of their personal data?
   a. Can we still provide a base product or service even if consent is not given?[2]
   b. Would users pay a premium to avoid the collection of their personal data?[3]
3. How autonomous is our IoT technology?
4. If we are required to pseudonymise our data, do our data lose any strategic value once they are pseudonymised? (For example, what value would be lost if we lost geolocation data?)[4]
5. How interoperable is our IoT technology with other third-party IoT technologies?[5]
6. How effectively can we contractually transfer the risks we incurred by our IoT-related activity to other parties, including insurers?
7. How does the way we price our products/services change based on our IoT technology's capabilities and/or the data we collect from users of our IoT technology?
8. Is the critical infrastructure in place in the jurisdiction(s) in which we operate to support our IoT technology?[6]
9. What risks do we incur because our IoT technology collects new types of data that we have not previously collected?
10. Have we sought legal advice regarding the high-level considerations listed in this checklist, particularly regarding the European Union's (EU's) General Data Protection Regulation (GDPR) and other relevant laws and regulations?

II. Preparing Our Company for the IoT

1. How are we acquiring the requisite talent to integrate the IoT into our business processes?
2. How are we training our employees and providing them with the skills necessary to integrate the IoT into our business processes?
   a. Is our training available and applicable to all employees in our company, including non-IT employees?[7]
3. How are we determining what data our IoT technology currently collects and the best uses of those data?
   a. What pre-emptive steps are we taking to mitigate the potential negative impact from these data?
4. What steps are we taking to culturally and financially support IoT initiatives within our company?

III. Implementation of IoT Initiatives

1. What IoT initiatives have we already integrated or will integrate into our processes?[8]
   a. Are we first proving the value of these IoT initiatives before we become concerned with scaling them?[9]
   b. Are we properly documenting these IoT initiatives?
   c. Are we evaluating these IoT initiatives through the use of clear business objectives, outcomes and metrics?
   d. Are they subject to the same performance expectations as other initiatives?
2. If our IoT initiatives are failing, why?[10]
   a. Is there collaboration between the IT side and the business side?
   b. Do we have a technology-focused culture, which is driven and led by senior leadership?
   c. Do we have access to internal and/or external IoT expertise?
   d. Do we have "ecosystem partnerships" with other entities at every phase of our initiatives, "from strategic planning to data analytics after rollout"?[11]
   e. Do our company's business strategy decision makers place as much importance on technology as our IT strategy decision makers?
   f. How are we learning from our failures?
3. Have we considered these five challenges at every stage of implementation?[12]
   a. Time to completion
   b. Limited internal expertise
   c. Quality of data
   d. Integration across teams
   e. Budget overruns

IV. Data Collection Considerations[13]

1. How do we treat B2B data differently than B2C data?
   a. Should we treat and protect B2B data in a different manner than B2C data?
2. Do we protect different types of data differently, such as personal data versus non-personal data?[14]
3. Do we have the resources and infrastructure to collect, retain and analyse the data collected from our IoT initiatives?
4. How are we confirming the accuracy of data collected from our IoT initiatives?
5. How are we adhering to the relevant data privacy and protection laws and regulations, including the GDPR?
   a. How are we adhering to data retention and data deletion laws and regulations, especially keeping in mind they may be discoverable in a court of law?
6. How are we working with labour unions and other entities intended to protect the data rights of our employees and other users?
7. If we no longer need to trace data back to individual users, can we anonymise the data collected from our IoT initiatives?[15]
8. If we still need to trace data back to individual users, can we pseudonymise the data to reduce the risk to users in the event of a data breach?

V. Industry and Sector Considerations

1. Under which industry(ies) and sector(s) do our IoT initiatives fall?
    a. What industry- and/or sector-specific considerations, such as specific regulations, do we have regarding our IoT initiatives?[16]
    b. What self-regulatory practices regarding IoT technology are companies in our industry or sector expected to follow?

VI. Tax Considerations

1. How do we determine in which jurisdiction(s) the profits generated from our IoT initiatives' data should be taxed?[17]
2. Are we now gathering data from more jurisdictions by virtue of our IoT initiatives?

VII. Trust and Human Impact Considerations

1. Is our IoT technology "trusted, accepted, wanted, accessible and usable" by users? (In other words, are people reluctant to use our IoT technology because of certain features or capabilities of our IoT technology?)[18]
2. How do we ensure that users understand how our IoT technology impacts their lives, especially if they do not have specific knowledge of the underlying technologies?[19]

VIII. Ethical and Discriminatory Considerations

1. Are we using our IoT technology to evaluate users in some manner? (For example, are we using telematics to determine whether users are good or bad drivers?)
    a. If yes, are we required to or should we be transparent in how such evaluations are made?
    b. If yes, does our evaluation process incentivise "bad actors" to behave in an unreasonable or improper manner?
    c. If yes, is there a risk that users behaving properly will be unfairly punished through a price increase or general decrease in options?
2. How often are we conducting an ethical audit to ensure that our IoT technology is not exhibiting discriminatory tendencies towards users or third parties?[20]

Contract and Tort Liability

I. Breach of Contract

1. What duties have we incurred regarding users because of the terms of use in the contract associated with our IoT technology?
2. What duties have we incurred due to the IoT nature of our technology?
    a. Have we not yet foreseen any of these duties or are any of these non-contractual duties?
3. Should we reasonably expect users to follow all contractual requirements and the terms of use concerning our IoT technology? (For example, is it reasonable to expect drivers of our autonomous vehicle to still pay attention while the vehicle is in autonomous mode)
4. Can our IoT technology purport to contract with another person, entity, or IoT technology on our behalf? (For example, can a smart refrigerator automatically place an order for more milk when the user is low on milk?)[21]
    a. If yes, how do we monitor and control such contracting capabilities, ensuring that we prevent unintended consequences such as over-ordering from vendors?[22]
5. Do we have any contractual responsibility for data our IoT technology possesses without regard to actual knowledge of humans in our company?[23]
6. Are we exposed to liability for the "loss or corruption of data arising in relation to" our IoT technology?[24]
7. How effectively can we disclaim all duties, such as a duty of care or duty to warn, through contracts or non-contractual disclaimers?

II. Terms of Contracts with Third Parties (Non-Users of IoT Technology)

1. How do we collaborate with third parties and ensure that the data we share with them are sufficiently protected, kept confidential, only used for the intended purposes and are the actual data requested by the third parties?[25]
2. How are we assessing the strength of the data protection and cybersecurity measures of the third parties with whom we contract?
    a. How do we ensure that these third parties are keeping up-to-date with their data protection and cybersecurity measures?
    b. How do we know when these third parties have been hacked?
    c. Can we identify the "weakest link in the chain"?
3. What, if any, terms on interoperability and security standards do our contracts involving our IoT technology include?[26]

Cybersecurity[27]

I. Keeping Abreast of Relevant Laws, Regulations and Standards

1. How are we keeping abreast of IoT-related developments in cybersecurity strategies and policies amongst the following organisations and standards?
    a. The European Union (EU), particularly the European Union Agency for Network and Information Security (ENISA)[28]
    b. Industry information sharing associations such as the Information Technology-Information Sharing and Analysis Center (IT-ISAC)[29]
    c. Information and communication technology (ICT) standards[30]
    d. International Organization for Standardization (ISO), particularly the ISO/IEC 27000-series on information security management[31]
2. [For the UK] Have we considered Cyber Essentials[32], a government-backed cybersecurity certification scheme, as a method of ensuring that we are adhering to our industry's best practices regarding cybersecurity?

II. General Considerations

1. How do our design, manufacturing, testing and maintenance processes coordinate to address cybersecurity issues?[33]
2. How are we ensuring that there are robust and clear security specifications regarding our IoT technology?[34]
   a. How are we ensuring that these specifications are followed throughout the entire lifecycle of the development and deployment of our IoT technology?
   b. Do we need to hire an IoT managed security services provider (MSSP) to manage our IoT-related cybersecurity?[35]
   c. What intrusion detection systems do we have in place?[36]
   d. How are we considering the security of all communication links, storage infrastructure, and other inputs of the ecosystem related to our IoT technology?[37]
3. Does our IoT technology require periodic software, firmware and/or hardware updates to fix any discovered security vulnerabilities?[38]
4. What training must we provide to our employees to ensure the relevant employees follow proper cybersecurity practices related to our IoT technology?
   a. Is that training designed for all employees, including non-IT employees?[39]
   b. How do we make employees aware of new cybersecurity threats?
5. How is our IoT technology considered in the context of our cybersecurity incident response plan(s)?
   a. Have we stress-tested our plan(s) to ensure it is effective in the context of an adverse cybersecurity incident affecting our IoT technology?
   b. Who on our incident response team has sufficient knowledge and understanding of our IoT technology?

III. Cybersecurity Breach

1. What are the financial and reputational costs of a cybersecurity breach?
2. Have any IoT technologies similar to ours that are owned or used by other companies been hacked?
   a. If yes, were these hacks malicious or done in a controlled environment?
   What was the result?
   b. How are we using the knowledge of these breaches to secure our own IoT technology?

IV. Username and Password

1. Does our IoT technology come with a default username and password?[40]
   a. If yes, can we provide users with unique default usernames and passwords?
   b. If yes, can we require them to change their default usernames and passwords to unique usernames and passwords?
2. Do we require multi-factor authentication for our IoT technology?[41]

General Data Protection Regulation (GDPR)

I. Determining Whether the GDPR Applies to Our IoT Technology

1. To determine whether we are a data controller[42] and/or data processor[43] and whether the GDPR applies, how are we considering the following?
   a. Do we control or process[44] personal data[45] of data subjects from the European Union (EU) or European Economic Area (EEA)[46] electronically or in any other organised way?[47]
      i. Do we control or process pseudonymised data rather than anonymised data?
      ii. Even following a pseudonymisation[48] exercise, can the personal data we control or process be linked or attributed to a data subject through the use of additional information?[49]
   b. Even if we are not established in the EU or EEA, do we control or process personal data of data subjects from the EU or EEA and carry out processing of personal data related to either of the following?[50]
      i. Offering goods or services to EU/EEA data subjects, regardless of whether we require payment from those EU/EEA data subjects;[51]
      ii. Monitoring the behaviour of data subjects that takes place in the EU/EEA[52]
2. Do we process personal data wholly or partly by automated means? Or, even if not processed by automated means, do the data form part, or are intended to form part, of a filing system?[53]
3. Does the jurisdiction(s) in which we operate have any exemptions, derogations, conditions or rules related to the GDPR?[54]

II. Collection of Personal Data

1. How does our IoT technology collect and process personal data?
   a. Are users of our IoT technology aware of the data collection and processing?
2. Does the operation of our IoT technology involve the processing of personal data relating to the following categories so that data subjects are personally identifiable?
   a. Race or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, health or biometric data, data concerning a data subject’s sex life or sexuality[55]
3. Does the operation of our IoT technology involve the processing of any data relating to criminal convictions?[56]

III. Data Protection Principles and Purpose Limitation

1. At the time we collect personal data from data subjects, do we provide them with complete information about exactly what personal data our IoT technology is collecting and for what purposes?[57]
2. Do we have a specific, explicit, lawful and legitimate purpose for collecting personal data?[58]
3. Do we limit our collection of personal data to that which is “adequate, relevant and limited to what is necessary” for the purpose of processing?[59]
4. Do we make sure that the personal data we collect and keep are accurate and kept up-to-date?[60]
5. Do we erase or update personal data quickly when requested by data subjects or if we discover the data are inaccurate?[61]
6. Do we keep personal data for no longer than is necessary?[62]
7. Do we carry out any automated decision-making or profiling activities such as an automated assessment of eligibility to use our IoT technology?[63]
   a. How do we inform data subjects of this automated decision-making or profiling?
   b. Can we offer data subjects the option to have the decision carried out by a human rather than by automated means if requested?

IV. Data Protection by Design

1. Do we consider data protection issues at the beginning of any project involving our IoT technology, including when we design and create our IoT technology?[64]
2. Do we include data security measures in the design of our IoT technology?

V. Cybersecurity

1. Do we use appropriate security mechanisms to protect the personal data that our IoT technology collects?[65]
2. Do we use appropriate technical and organisational measures to ensure that personal data are kept secure?[66]

VI. Transparency and Information to Provide to Data Subjects

1. If we are the data controller, how do we provide the following information to data subjects when we collect personal data?[67]
    a. The identity and contact details of the data controller and the data protection officer[68]
    b. How to contact us to make requests and exercise their rights in relation to their personal data and our processing activity[69]
    c. The purpose, nature and legal basis of processing[70]
        i. What do we rely on as our legal basis for processing? Is it consent, legitimate interests, the requirement for the performance of a contract or another legal basis?
        ii. Do we carry out automated processing?
    d. Details of any other organisations to which we will send the personal data[71]
    e. For how long we will keep the personal data[72]
    f. Details of any transfer of personal data outside the EU/EEA
    g. Whether data subjects need to provide their personal data to meet a contractual requirement, statutory requirement, consent requirement or other legitimate interest, and what will happen if they do not provide the personal data[73]

VII. Using Personal Data for Other Purposes and Obtained from Other Sources[74]

1. If we want to use personal data for a reason other than the reason for which we originally collected them, such as using registration data to operate another function of our IoT technology, do we give data subjects all of the information listed in the section titled "Transparency and Information to Provide to Data Subjects" above?
2. Do we use personal data that we have obtained by third parties and not from data subjects?[75]
    a. If yes, do we provide data subjects with the information set out in the section titled "Transparency and Information to Provide to Data Subjects" above? Or do we ensure that the third party has provided this information and obtained all relevant consents/authorisations required to enable us to process the personal data for our purposes?

VIII. Consent Requirements[76, 77]

1. How do we obtain consent[78] from data subjects to carry out processing of personal data?
    a. Do we keep records of consents given and the relevant consent wording?
    b. Do we need "explicit" consent?[79]
2. Is the request for consent that we send to data subjects separate from our other requests for information such as agreeing to our terms and conditions?
    a. Is our request for consent written using clear and plain language, and is the consent clearly given? (In other words, do data subjects need to tick a box or give another clear indication that they give consent?)[80]
    b. May data subjects use our IoT technology without giving consent?[81]
3. If consent is required to process data, what procedures do we have in place to allow data subjects to withdraw their consent to such processing?[82]
    a. Is it as easy for data subjects to withdraw consent as it is for them to give consent? (For example, can we provide an "unsubscribe" link in all marketing emails?)

IX. Children's Consent[83]

1. Have we considered whether children will use our IoT technology and whether they will need to consent or require parental consent?[84]

X. Accountability

1. Can we demonstrate "accountability" through our compliance with the data protection principles enumerated in Article 5(1) of the GDPR?[85]
    a. Do we keep accurate and comprehensive written records regarding data protection matters?[86]
2. Do we act in accordance with the requirements in Chapter IV of the GDPR? (See Appendix C: Requirements Included in Chapter IV of the GDPR for Data Controllers and Data Processors for some requirements.)
3. What training do we provide our employees on how to handle any requests from data subjects about exercising their rights in connection with their personal data?

XI. Rights of Data Subjects Regarding Their Personal Data

1. How are we providing data subjects with reasonable and timely notice regarding their rights to the following? (See Appendix D: Rights of Data Subjects Regarding Their Personal Data for a detailed analysis of the following.)
    a. Access
    b. Rectification (correcting incorrect data)
    c. Erasure ("right to be forgotten")
    d. Restriction of processing
    e. Data portability
    f. To object to processing

XII. Arrangements with Data Processors

1. Are we, as a data controller, adhering to the responsibilities of a controller?[87]
2. Are we, as a data processor, adhering to the responsibilities of a processor?[88]
3. Do we appoint third parties to process personal data on our behalf?
    a. If yes, do we include the mandatory provisions enumerated in Article 28 of the GDPR in our contracts with those third parties?

XIII. Cross-Border Data Transfers

1. Are we in compliance with the GDPR's requirements regarding cross-border data transfers?[89]
   a. Do we have adequate safeguards to protect the personal data in place?[90]
   b. How do we provide data subjects with details of any transfers of personal data to another country and the safeguards that will be used to protect personal data?

XIV. Data Breaches

1. What procedures do we have in place to enable us to notify the relevant supervisory authority(ies) about a data breach (and to provide information such as the type of personal data and number of data subjects concerned) within 72 hours of becoming aware of the data breach?[91]
2. What procedures do we have in place to document information about data breaches, including remedial action and effects of the data breach?
3. Do we have procedures in place to quickly inform data subjects of a data breach if the data breach would result in "high risk" to those data subjects such as if data subjects' payment details are involved?[92]

XV. Enforcement, Sanctions and Remedies

1. What are the potential enforcement mechanisms, sanctions and remedies available to national regulators and data subjects whose personal data we collect and/or process?[93]

Other Data Protection Considerations

I. Article 29 Working Party (WP29)

1. How are we keeping abreast of any materials published by the WP29?[94]

II. Other Directives

1. What other EU directives apply to our IoT-related activity, and how are we ensuring that we are compliant? For example, how are we considering the following?
   a. NIS Directive[95]
   b. Regulation on Privacy and Electronic Communications (ePrivacy Regulation)[96]
      i. (Please note that the ePrivacy Regulation was pending at the time this checklist was drafted, but the Regulation may impose significant responsibilities regarding IoT technology that should be considered.)
   c. Directive (EU) 2016/680[97]
   d. Directive (EU) 2016/681[98]

III. Local Data Protection Authorities

1. How are we keeping abreast of any guidance published by local data protection authorities?

IV. Working with Standardisation Bodies

1. Are we, or our trade associations or vendors, working with standardisation bodies to:
   a. Create a "common protocol to express preferences with regard to data collection and processing by data controllers"?[99]
   b. "[D]evelop lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentiality, integrity, authentication and access control"?[100]

V. Data Residency

1. In which jurisdiction(s) does our data reside?
   a. Do we create a data map to understand where our data reside?[10]1
2. At any time, do our data leave the jurisdiction(s) in which we operate?
   a. If yes, in what format do our data leave?
   b. Are other entities, such as subcontractors, able to take our data out of the jurisdiction(s) in which we operate without our knowledge or consent?
3. Do we have data residency provisions in our relevant contracts that delineate where data may reside?
   a. How are we informing users and other relevant parties about where our data reside?
4. Do the data remain in the IoT technology or in another local technology? Or are the data transmitted to the cloud or a remote, centralised location?
   a. If data are stored in the cloud, how does our cloud strategy support our data protection and data residency protocols?
   b. If data are stored in the cloud, are they encrypted in transit and at rest?

VI. Data Ownership

1. Who owns the data that our IoT technology is collecting from data subjects?[102]
   a. Data subjects
   b. Data controller
   c. Data processor
   d. Other
2. Who has access or usage rights to the data that our IoT technology is collecting?
   a. Are we licenced to use the data if we do not own them?
   b. If we own the data and grant third parties the rights to use them, do such licences protect our rights in the data?
3. How do we separate personal data from non-personal data?[103]
4. Does the timing of when data are collected help determine whether the data may be collected? (For example, can we collect our employees' geolocation data at all times but are only permitted to do so during working hours?)
5. Do we apply various levels of importance to different types of data?[104]

VII. Business Confidential Data

1. Is our IoT technology collecting business confidential data, such as blueprints, the status of physical assets, etc.?
   a. How are we protecting these data? Are we protecting these data in the same manner as we do with data subjects' personal data per the GDPR?

VIII. Data Repurposing

1. Is pseudonymisation of data subjects' personal data sufficient or do we need to anonymise?
2. What inferences can third parties draw from the data collected by our IoT technology? (For example, can inferences be made regarding data subjects' consumer preferences?)[105]

IX. Bystanders' Personal Data

1. What rights of access and opposition regarding their personal data do bystanders possess?[106]
    a. How do those rights compare to users of our IoT technology?
    b. Do bystanders' rights vary based on whether they have a contractual relationship with users of our IoT technology?[107]
    c. Do users of our IoT technology incur a duty to notify bystanders of the collection of the bystanders' personal data?[108]
        i. Do users incur a duty to respect bystanders' preferences not to have their personal data collected by our IoT technology?[109]
    d. Are we able to distinguish personal data collected from users and bystanders?

X. Free Flow of Data

1. How are our data both internally and externally accessible?[110]
2. Can we control the flow of data collected by our IoT technology?[111]

Intellectual Property (IP)

1. Have we approached our in-house counsel regarding the following IP considerations related to our IoT technology? (See Appendix E: Intellectual Property (IP) for a detailed analysis of the following.)
    a. Licensing our IP
    b. Licensing third-party IP
    c. Protecting our data with IP

Liability Assignment Amongst Multiple Parties

I. General

1. Is our IoT technology a product or a service?[112]
    a. Do we understand the legal implications and responsibilities of each and how they differ from one another?

II. Determining Product Liability Regime[114]

1. Does our IoT technology operate under a strict liability regime, which means that parties may be held liable regardless of whether they were at fault?[113]
2. Does our IoT technology operate under a negligence regime, which means that parties must be at fault to be held liable?

III. Liability Assignment

1. What entities are involved in the ecosystem of our IoT technology?[115]
    a. Product manufacturers
    b. Sensor manufacturers
    c. Software producers
    d. Infrastructure providers
    e. Internet providers
    f. Maintenance providers
    g. Data analytics companies
    h. End users
    i. Third-party technologies and service providers
    j. Others

2. If there is personal injury or property damage, how do we determine if our IoT technology is responsible?
    a. If our IoT technology is responsible, how is liability assigned?[116]
        i. Which entity(ies) in the ecosystem is likely to be held fully or partially liable?
        ii. Are we able to contractually delineate responsibility if such an event were to occur?[117]
3. Which entity(ies) is responsible for ensuring the safety of our IoT technology initially and on an ongoing basis?[118]
4. What are the interdependencies and interoperabilities between our IoT technology and both service providers and other products?[119]
5. If our IoT technology is a system, how are we keeping abreast of any IoT-related updates to the European Union's Directive 2000/31/EC and other directives relating to e-commerce or information society services that could be applicable to our IoT system?[120]

Product Liability

I. Keeping Abreast of Relevant Laws, Regulations and Standards

1. How are we keeping abreast of any IoT-related updates to the EU's Product Liability Directive 85/374/EEC (PLD or Defective Product Directive)[121], the Machinery Directive 2006/42/EC (MD)[122], the Radio Equipment Directive 2014/53/EU (RED)[123] and other directives that could be applicable to our IoT technology?
    a. Have the Product Liability Directive and Machinery Directive been updated based on planned evaluations, which were intended to verify whether these Directives needed to be adapted to meet the needs associated with the IoT?[124]
    b. If our IoT technology is subject to RED, are we aware of the essential requirements for radio equipment within certain categories or classes?[125]
2. Do we understand that the Product Liability Directive, Machinery Directive and Radio Equipment Directive can be applied to "provid[e] a thorough legislative framework for the safety of" autonomous systems within the IoT?[126]
3. How are we keeping abreast of any IoT-related updates to standards created by the International Organization for Standardization (ISO), including the following, as they are adopted by the EU?[127]
    a. ISO 12100:2010, Safety of machinery – General principles for design – Risk assessment and risk reduction[128]
    b. ISO 10218-1:2011, Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots[129]
    c. ISO 10218-2:2011, Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration[130]
    d. ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design[131]
    e. ISO 13482:2014, Robots and robotic devices – Safety requirements for personal care robots[132]
4. For the jurisdiction(s) in which we operate, are there any product safety standards and certifications to which we must adhere?

II. Our Own Understanding of Our IoT Technology and Its Use

1. Do we understand the capabilities of our IoT technology?
    a. Is it "dumb" technology, which has connectivity and execution capabilities but is not self-determining? (An example would be a door lock that is controlled over the Internet.)[133]
    b. Is it self-determining artificial intelligence (AI) technology with ambient intelligence[134] and autonomous control?[135]
        i. If yes, are there "certain minimum ethical standards" to which the use of our IoT technology must adhere for it to be socially accepted?[136]
2. Does our IoT technology have the capability to exhibit unexpected and unintended behaviour that could cause personal injury and/or property damage?[137]
3. How do we define "defect" regarding our IoT technology, especially if it is self-learning?[138]
4. How likely is it that our IoT technology will collect erroneous data due to, for example, "software defects, connectivity problems or incorrect operation of the [technology]"? [139]

III. Users' Understanding of Our IoT Technology and its Use

1. How well do users understand the capabilities of our IoT technology?
    a. Per the General Product Safety Directive 2001/95/EC (GPSD) and Product Liability Directive, how are we providing adequate instructions and warnings to users so they can safely use our IoT technology?[140]
2. How are users using our IoT technology and is that the intended use?
    a. How foreseeable is it that users would use our IoT technology in a manner that we did not intend?
3. How easy is it for users and bystanders to recognise that our IoT technology is IoT in nature?[141]

IV. Designing and Manufacturing Our IoT Technology

1. Do we meet our industry's best practices in the design and manufacturing processes of our IoT technology, especially to ensure product safety and security?
2. How are we documenting our design and manufacturing processes?
3. Was our IoT technology always intended to be IoT in nature?
    a. If no, how do we ensure that all steps are taken to properly transition the technology to being IoT in nature?
4. Does our IoT technology need to be IoT in nature?
5. How is cybersecurity considered when our IoT technology is being designed?
6. Does our IoT technology create a risk for personal injury and/or property damage?
    a. If yes, can we design out all of or some of the risk with reasonable modification?
7. How specifically do users benefit if we improve the design of our IoT technology to reduce the risk of personal injury and/or property damage?
8. What interoperability requirements does our IoT technology have?[142]
    a. Is there a standardisation by which we must adhere?[143]
    b. Which standard-setting bodies should we be following to determine the interoperability technical standards for our IoT technology?[144]
9. Does our IoT technology have a power save or sleep mode?
    a. If yes, what is the risk that when our IoT technology is in power save mode, it will miss an event that would typically trigger an alert?
10. Is our IoT technology battery powered?
    a. If yes, how are we informing users of how long our IoT technology will typically last without being recharged or the battery replaced?[145]
11. What critical city, regional and/or national infrastructure is necessary for our IoT technology to properly operate?

V. Updates

1. What industry or jurisdictional requirements exist that require us to make updates to our IoT technology?
2. How often are we updating our IoT technology, especially to mitigate the risk of hacks or involuntary releases of personal data?
    a. Are we updating as frequently as is standard in our industry?
3. How are the updates made?
    a. Can the updates be made automatically without user consent or do they require user consent?
        i. If user consent is required, how easy is it for users to make the updates?
4. Are the updates for our IoT technology recommended to users or required of users?
    a. Can we legally require users to update our IoT technology?
5. What kinds of updates do we make? Do we make software, firmware, and/or hardware updates?
6. How do we know if an update fails and how do we notify users that the update failed?
7. What other responsibilities to maintain our IoT technology do we incur?
8. For how long should our IoT technology be in service before becoming obsolete and no longer updated?

VI. Testing Our IoT Technology: Pre-Market Testing

1. What testing procedures, particularly cybersecurity testing, are completed before our IoT technology goes to market?
    a. What internal and/or external expert input do we receive before our IoT technology goes to market?
    b. Are we hiring computer security experts, such as “white hat” hackers[146], to try to hack into our IoT technology?
        i. If yes, what has been the result of their efforts to hack into our IoT technology?
            (a). If they have successfully hacked into our IoT technology, have we identified and eliminated the vulnerabilities?
        ii. Do we meet our industry’s best practices in the testing of our IoT technology?
        iii. How are we documenting our testing processes?
        iv. What quality assurance and testing are we performing to decrease the risk of erroneous data being collected by our IoT technology?147

VII. Testing Our IoT Technology: Ongoing Testing

1. What pre-market testing considerations are applicable after our IoT technology goes to market? (See the section titled “Testing Our IoT Technology: Pre-Market Testing” above.)
2. How regularly are we testing our IoT technology?[148]
3. When risks pertaining to our IoT technology are identified, what are our follow-up testing procedures?
    a. How do we use the testing results to update our IoT technology?

VIII. Providing Notice, Warning and Instructions

1. How do we identify the users of our IoT technology?
    a. Are we reasonably able to physically contact those users?
2. How are we providing reasonable and timely notice to users regarding the following, paying particular attention to the requirements enumerated in the General Product Safety Directive 2001/95/EC (GPSD)?[149]
    a. When there is an emergency either related to or recognised by our IoT technology
        i. When appropriate, does our IoT technology automatically alert emergency personnel?
    b. When there is an update to the software, hardware and/or firmware of our IoT technology
    c. When a security vulnerability is discovered in our IoT technology
    d. When our IoT technology is discovered to be at risk for causing personal injury and/or property damage
    e. When our IoT technology becomes obsolete and will no longer be updated
3. How often are we reminding users that our IoT technology is collecting their personal data?[150]
4. How are we instructing users on how to keep their IoT technology secure?
5. Have we incurred a legal duty to warn users of potential risks of personal injury and/or property damage?
    a. Can we disclaim responsibility to provide such warning?
    b. If we have incurred such a duty to warn, how do we provide users with reasonable and timely notice?
        i. Does that duty to warn extend to any unintended recipients such as third-party users or bystanders?
    c. Have we incurred a legal duty to take steps to protect those users and their property through the mitigation or elimination of those potential risks?
        i. If yes, what are those required steps?
            (a). Do those steps involve notifying a third party(ies), such as emergency personnel, in the user's behalf if the user is physically or mentally unable to receive and heed a warning?

IX. Protective Measures

1. What safety features are the users of our IoT technology "entitled to expect, taking all circumstances into account"?[151]
2. Does our IoT technology possess a "kill switch" that allows it to be turned off by users or by us, especially when it is obsolete or at risk for causing personal injury and/or property damage?[152]
3. How are we preventing our obsolete IoT technology from being used for malicious purposes?

X. Users' Responsibilities Regarding Our IoT Technology

1. What responsibilities do our users incur regarding the maintaining and updating of our IoT technology?
    a. How are we providing users with reasonable and timely notice of such responsibilities?
    b. Do any of these responsibilities relate to third-party users and/or bystanders?

XI. Enforcing Responsibilities of Third Parties

1. How do our responsibilities in this Product Liability section apply to third parties who are involved in the lifecycle of our IoT technology?
    a. How do we enforce the applicable responsibilities?

Appendix

Appendix A: Overview of Consent per the General Data Protection Regulation (GDPR)[153]

Asking for Consent

1. Have we "checked that consent is the most appropriate lawful basis for processing"?
2. Have we "made the request for consent prominent and separate from our terms and conditions"?
3. Do we "ask people to positively opt in"?
4. Do we refrain from using "pre-ticked boxes, or any other type of consent by default"?
5. Do we "use clear, plain language that is easy to understand"?
6. Do we "specify why we want the data and what we're going to do with it"?
7. Do we "give granular options to consent to independent processing operations"?
8. Have we "named our organisation and any third parties"?
9. Do we "tell individuals they can withdraw their consent"?
10. Do we "ensure that the individual can refuse to consent without detriment"?
11. Do we refrain from making "consent a precondition of a service"?
12. "If we offer online services directly to children, [do] we only seek consent if we have age-verification and parental-consent measures in place"?
13. Do we accept consent from legal guardians of those who are physically or mentally unable to provide proper consent?

Recording Consent

1. Do we "keep a record of when and how we got consent from the individual"?
2. Do we "keep a record of exactly what they were told at the time"?

Managing Consent

1. Do we "regularly review consents to check that the relationship, the processing and the purposes have not changed"?
2. Do we "have processes in place to refresh consent at appropriate intervals, including any parental consents"?
3. Do we "consider using privacy dashboards or other preference-management tools as a matter of good practice"?
4. Do we "make it easy for individuals to withdraw their consent at any time, and publicise how to do so"?
5. Do we "act on withdrawals of consent as soon as we can"?
    a. Do we inform other IoT stakeholders involved as soon as individuals withdraw consent or oppose data processing?[154]
6. Do we refrain from "penalis[ing] individuals who wish to withdraw consent"?

Appendix B: Cybersecurity per the European Union Agency for Network and Information Security (ENISA)[155]

1. What countermeasures do we have in place to address accidents or intentional attacks?
2. Regarding good practices to address accidents:
    a. Monitoring of KPIs: How are we monitoring key performance indicators (KPIs) (e.g., temperature, output, response, connectivity, etc.) to "determine if hardware is operating within accepted parameters" and/or to better "identify the early onset of issues"?

    b. Hardware redundancy: Do we have hardware redundancy with all of our vital hardware?

    c. Shutdown procedures: What are our shutdown procedures in place to either disable or deactivate our IoT technology?

    d. Design specifications: Do our design specifications "integrate security requirements" beginning in the first stages of the design?

    e. Maintenance scheduling: Does our maintenance schedule aim to maximize availability and mean time "between equipment failures, at the least cost"?

        i. Does our maintenance schedule facilitate "the early detection of potential malfunctioning or failure"?

    f. Response teams: Do we have a trained response team who are prepared for and respond to emergency incidents?

    g. Quality assurance: Do we have quality assurance to "prevent[] mistakes or defects in [our] manufactured" IoT technology?

    h. Reporting procedures: Do we have procedures on how to report an incident and are those procedures written for all levels of our company and not just the technical staff?

        i. Do these procedures "provide guidance on 'what to report', 'who to report', and 'how to report'"?

    i. Debugging procedures: Do we have procedures for troubleshooting specific software errors?

    j. Maintenance of backups: Do we "[m]aintain backups of data, ideally in secure off-site servers that allow for data recovery in the case of corruption/loss"?

    k. Creation of activity logs: Do we maintain activity logs, audit trails, and error logs that indicate what happened when an incident occurs?

        i. Are these logs regularly backed up safely (e.g., remotely with encryption)?

    l. Regular auditing: Do we regularly inspect our infrastructure (digital and/or physical) to "evaluate [and/]or improve its appropriateness, safety, efficiency, or the like"?

        i. Do these audits provide reports pointing out weaknesses and vulnerabilities, proposing remedial actions?

    m. Operator/user training: How are we training our employees/users on how to use the cybersecurity processes related to our IoT technology?

    n. Awareness raising: How do we inform employees/users of our IoT technology to new and existing threats?

    o. Standard operating procedures: What are our standard operating procedures regarding, "for instance, incident reporting or response"?

    p. Response procedures: What are our response procedures to incidents? Do they include the processes "to follow (what to do), the reporting chain (who to report to) and define minimum KPIs for service recovery (e.g., degraded mode)"?

    q. Diagnosis of hardware/software faults: Do we have a "[s]ystemic approach towards the diagnosis of hardware and software faults"?

    r. Encryption of data: How are we encrypting sensitive data?

    s. Access control: What access controls do we have in place to prevent any unauthorised access?

t. Continuous security monitoring: What continuous security monitoring methods do we use, including passive network monitoring and active network scanning, "to detect any impact on the security requirements via either a set of predefined rules or real-time analysis"?

u. Implementation of an information security policy: Have we implemented an information security policy to manage the security of information related to our IoT technology throughout our organisation?

v. Incident reporting system: Do we have reporting systems focused on critical incidents that monitor KPIs "and trigger alarms when the service or security requirements are not met"?[156]

w. Use of open design hardware/software: Do we use open design hardware/software, which "is the development of physical products, machines and systems through use of publicly shared design information," "when the redevelopment of certain functionalities is a security risk (e.g., encryption)"?

x. Defined terms of support: Do we have clearly defined support levels that enumerate the roles of every actor (e.g., operator, contractor, etc.) and the liabilities in case of a security incident?

y. Regular infrastructure upgrade: Are we making regular software and/or hardware upgrades to our infrastructure "to prevent obsolescence and overcome vulnerabilities found after a risk assessment"?

z. Surge protections: Do we use surge protectors designed to protect electrical devices essential to the service from voltage spikes?

aa. Increase resilience: How are we "[i]ncreas[ing] resilience by reducing "single points of failure" to critical systems?[157]

bb. Remote deactivation of device capabilities: Can our IoT devices be remotely deactivated either "directly at devices level with secure remote access or at the supervisory system level"?

cc. Emergency maintenance teams: Do we have emergency maintenance teams that can "recover a minimum service in a limited time"?

dd. Device hardening: Are we sufficiently hardening our systems?

ee. Enhanced engineering requirements: Are we "carefully defining, documenting and maintaining [enhanced engineering] requirements," and are they "drafted within the objectives of the service and with quantifiable key performance indicators"?

ff. Early warning systems/forecasting: Do we have "[e]arly warning systems [that] actively involve the communities at risk, facilitate awareness of risks, effectively disseminate alerts, and ensure there is a constant state of preparedness"?

gg. Disaster recovery processes/centres: Do we have a disaster recover plan "to recover operations in the event of a disaster"?

hh. Infrastructure threat assessments: Do we have a "[f]orm of assessment to evaluate the risk an infrastructure is exposed to," and is it a "prerequisite to any further action"?

3. Regarding good practices to address intentional attacks:

a. Use of virtual private networks: Do we have a virtual private network that "extends a private network across a public network and allows benefiting from the functionality, security and management policies of the private network"?

b. Encryption of data: How are we encrypting sensitive data?

c. Deploy network intrusion detection systems: Do we have a network intrusion detection system that "inspect[s] all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack"?

d. Deployment of physical protection: Do we deploy physical protection that "aims at limiting tampering and unauthorised access to the physical infrastructure," particularly for "equipment not located in a secure location"? Such measures "include locks, alarms, surveillance equipment, sensors, access control systems, etc."

e. Access control: What access controls do we have in place to prevent any unauthorised access?

f. Alarms and surveillance: Do we have alarms that "give a signal when a problem or a specific condition[] occurs," and surveillance that monitors "behaviour or other changing information"?

g. Implementation of an information security policy: Have we implemented an information security policy to manage the security of information related to our IoT technology throughout our organisation?

h. Creation of activity logs: Do we maintain activity logs, audit trails, and error logs that indicate what happened when an incident occurs?

   i. Are these logs regularly backed up safely (e.g., remotely with encryption)?

i. Maintenance of backups: Do we "[m]aintain backups of data, ideally in secure off-site servers that allow for data recovery in the case of corruption/loss"?

j. Regular auditing: Do we regularly inspect our infrastructure (digital and/or physical) to "evaluate [and/]or improve its appropriateness, safety, efficiency, or the like"?

   i. Do these audits provide reports pointing out weaknesses and vulnerabilities, proposing remedial actions?

k. Shutdown procedures: What are our shutdown procedures in place to either disable or deactivate our IoT technology?

Appendix C: Requirements Included in Chapter IV of the GDPR for Data Controllers and Data Processors

1. Appointing a data processor[158]
2. Appointing a data protection officer (DPO)[159]
3. Meeting documentation requirements for both data controllers and data processors[160]
4. Assessing the risk to data subjects' rights and freedoms[161]
5. Conducting a data protection impact assessment (DPIA), which is required before "undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes"[162]
6. Implementing data protection measures "by design and by default" when processing personal data such as through the use of pseudonymisation[163]
7. Signing up to a code of conduct or certification[164]
8. Implementing appropriate technical and organisational data security measures[165]
9. Assessing the appropriate level of security[166]
10. Implementing a breach notification system to notify the relevant regulator(s) and data subjects[167]

Appendix D: Rights of Data Subjects Regarding Their Personal Data

1. Notice of rights

   a. How do we inform data subjects on how to contact us to make requests and exercise their rights in relation to their personal data and our processing activity? (For example, do data subjects know how to ask us to correct erroneous data or to object to processing?)[168]

   b. What procedures do we have in place so we can quickly process any such requests from data subjects?

   c. How do we inform data subjects of their right to complain to the regulator in their jurisdiction such as the UK's Information Commissioner's Office (ICO)[169]?

2. Right to Access
    a. What procedures do we have in place to handle any access requests that data subjects may make?[170]
    b. What procedures do we have in place to locate personal data to respond within the deadline of 30 days from when access requests were made?
3. Right to Rectification (Correcting Incorrect Data)[171]
    a. What procedures do we have in place to quickly correct any data about a data subject if they ask us to do so?
4. Right to Erasure ("Right to Be Forgotten")[172]
    a. What procedures do we have in place to quickly delete data subjects' personal data if they ask us to do so?[173] [174]
5. Restriction of Processing[175]
    a. What procedures do we have in place to pause the processing of data subjects' personal data for a certain time if they ask us to do so?[176] [177]
6. Right to Data Portability[178]
    a. Are we easily able to provide an electronic copy of data subjects' personal data if they have given consent to permit us to process their personal data or if we carry out automated processing of their personal data and they ask us to send a copy of their personal data to another organisation?[179]
7. Right to Object to Processing[180]
    a. What procedures do we have in place to quickly respond to requests from data subjects who object to our processing of their personal data if we are processing their personal data:
        i. In connection with the "legitimate interests" of our organisation?[181]
        ii. In connection with any direct marketing we send to data subjects?[182]

Appendix E: Intellectual Property (IP)

General Considerations Regarding Our IoT Technology

1. Have we approached our in-house counsel regarding the following considerations? (Please note that many of the questions posed in this section are better suited for in-house counsel.)
2. What IP does our IoT technology implicate?
3. Who owns that IP and how is it licenced?[183]
4. Do we have all requisite licences for third-party components included in our IoT technology?
5. What open source IP does our IoT technology incorporate, if any? Do we intend on using other open source IP in relation with our IoT technology?[184]
    a. What are the terms of those applicable open source licences?
    b. What obligations do those applicable open source licences impose on us?
6. What non-disclosure agreements (NDAs) have we made with third parties regarding our IoT technology and how enforceable are they?
    a. What potential legal liabilities or risks to IP are not protected by the NDAs?

Protecting Our Data with IP

1. How are our data protectable by existing IP rights?[185]
    a. Do our data qualify as a "trade secret" under the Trade Secrets Protection Directive (2016/943/EU) (a.k.a., Trade Secrets Directive)?[186]
    b. Could our data be protectable under the Database Directive (96/9/EC)?[187]
    c. Could our data be protectable under the Copyright Directive (2001/29/EC)?[188]

Citations

[1] “InsurTech: where are they now?,” Norton Rose Fulbright, February 2017, http://www.nortonrosefulbright.com/knowledge/publications/146348/insurtech-where-are-we-now.

[2] We should ensure that consent is freely given. Conditional consents are not prohibited under the GDPR but are highly frowned upon.

[3] “Is Privacy Policy Language Irrelevant to Consumers?,” p. 9, Lior Strahilevitz and Matthew B. Kugler, September 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449.

[4] “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 15-16, Norton Rose Fulbright, February 2016.

[5] “Big Data: Protecting rights and extracting value,” p. 5, Norton Rose Fulbright, January 2015.

[6] “Advancing the Internet of Things in Europe,” p. 29, European Commission Staff Working Document, 19 April 2016.

[7] “Cyber security: How can the dial be turned from awareness to action?,” Roxanne Morison, 11 September 2017, https://www.linkedin.com/pulse/cyber-security-how-can-dial-turned-from-awareness-action-morison/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base%3BWECnc5zESGOUOKUolfTS1w%3D%3D.

[8] “Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing,” Cisco, 23 May 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1847422.

[9] Maciej Kranz’s *Building the Internet of Things, Implement New Business Models, Disrupt Competitors, Transform your Industry* offers an in-depth practice guide on how to implement the IoT into organisations.
http://www.maciejkranz.com/.

[10] “Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing,” Cisco, 23 May 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1847422.

[11] Cisco’s survey found that the companies with the most successful IoT projects “engage[d] the IoT partner ecosystem at every stage” of their IoT initiatives. “Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing,” Cisco, 23 May 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1847422.

[12] “Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing,” Cisco, 23 May 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1847422.

[13] “Big Data: Protecting rights and extracting value,” pp. 1-5, Norton Rose Fulbright, January 2015.

[14] It is recommended that we protect all data in the same or in a similar manner in order to avoid creating backdoors or other vulnerabilities for more sensitive data.

[15] Fully anonymised personal data falls outside the application of data protection legislation.

[16] “Big Data: Protecting rights and extracting value,” p. 6, Norton Rose Fulbright, January 2015.

[17] “Big Data: Protecting rights and extracting value,” p. 5-6, Norton Rose Fulbright, January 2015.

[18] “Advancing the Internet of Things in Europe,” p. 28, European Commission Staff Working Document, 19 April 2016.

[19] “Advancing the Internet of Things in Europe,” p. 28, European Commission Staff Working Document, 19 April 2016.

[20] “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 11, Norton Rose Fulbright, February 2016.

[21] Referred to as “automatic contracting” in “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 13, Norton Rose Fulbright, February 2016; “Advancing the Internet of Things in Europe,” pp. 22-23, European Commission Staff Working Document, 19 April 2016.

[22] “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 13, Norton Rose Fulbright, February 2016.

[23] Does our IoT technology have the capability to learn from the data it collects and can it act upon that data without human intervention or consent? Do we therefore incur a duty to warn users of our IoT technology’s capability?

24 “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 17, Norton Rose Fulbright, February 2016.

25 “Big Data: Protecting rights and extracting value,” p. 8, Norton Rose Fulbright, January 2015; “Building a European Data Economy,” p. 12, European Commission Staff Working Document, 10 January 2017.

26 “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 18, Norton Rose Fulbright, February 2016.

27 See also Appendix B: Cybersecurity per the European Union Agency for Network and Information Security (ENISA).

28 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity; See ENISA’s recommended good practices found in “Cyber security for Smart Cities: An architecture model for public transport,” pp. 33-37, European Union Agency for Network and Information Security (ENISA), December 2015, https://www.enisa.europa.eu/publications/smart-cities-architecture-model.

29 https://www.it-isac.org/.

30 “A Connected Digital Single Market for All,” p. 25, European Commission Staff Working Document, 10 May 2017.

31 https://www.iso.org/isoiec-27001-information-security.html.

32 https://www.itgovernance.co.uk/cyber-essentials-scheme.

33 “Cyber Security and Resilience of smart cars: Good practices and recommendations,” p. 57, European Union Agency for Network and Information Security (ENISA), December 2016.

34 “Cyber Security and Resilience of smart cars: Good practices and recommendations,” p. 58, European Union Agency for Network and Information Security (ENISA), December 2016.

35 https://www.i-scoop.eu/internet-of-things-guide/growth-iot-managed-security-services-market/.

36 “Big Data and the Internet of Things, Protecting rights, controlling use and extracting value”, p. 17, Norton Rose Fulbright, February 2016.

37 “Opinion 8/2014 on the Recent Developments on the Internet of Things,” p. 9, Article 29 Data Protection Working Party, adopted 16 September 2014.

38 “Who Makes the IoT Things Under Attack?,” Brian Krebs, 3 October 2016, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/.

39 “Cyber security: How can the dial be turned from awareness to action?,” Roxanne Morison, 11 September 2017, https://www.linkedin.com/pulse/cyber-security-how-can-dial-turned-from-awareness-action-morison/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base%3BWECnc5zESGOUOKUolfTS1w%3D%3D.

40 https://iconewsblog.org.uk/2016/07/15/public-must-act-to-protect-themselves-when-using-internet-of-things-devices/; “Who Makes the IoT Things Under Attack?,” Brian Krebs, 3 October 2016, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/.

41 https://iconewsblog.org.uk/2016/07/15/public-must-act-to-protect-themselves-when-using-internet-of-things-devices/.

42 Article 4(7), GDPR, defines “controller” as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

43 Article 4(8), GDPR, defines “processor” as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”

44 Article 4(2), GDPR, defines “processing” as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

[45] Article 4(1), GDPR, defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[46] The EEA includes all EU countries as well as Iceland, Liechtenstein and Norway.

[47] Article 3(1), GDPR; "Overview of EU General Data Protection Regulation," p. 2, Robbie Downing, 2017.

[48] The GDPR explains that data that have undergone pseudonymisation could still "be attributed to a natural person by the use of additional information" (Recital 26, GDPR). The GDPR also explains that "[t]he application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in [the GDPR] is not intended to preclude any other measures of data protection."

[49] Articles 5(1)(f) and 32, GDPR; See Recital 26, GDPR.

[50] "Overview of EU General Data Protection Regulation," p. 3, Robbie Downing, 2017.

[51] Article 3(2)(a); Recital 23, GDPR, explains "that the mere accessibility in the EU of the controller's, processor's or intermediary's website, an email address or other contact details, or the language generally used in the third country where the controller is established, is insufficient to ascertain that intention." However, if it is obvious that the online provider envisages to target EU data subjects, then the GDPR is likely to apply; "Overview of EU General Data Protection Regulation," p. 3, Robbie Downing, 2017.

[52] Article 3(2)(b), GDPR; "Overview of EU General Data Protection Regulation," p. 3, Robbie Downing, 2017.

[53] Article 2(1), GDPR; "Overview of EU General Data Protection Regulation," p. 3, Robbie Downing, 2017; A "filing system" is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis" (Article 4(6), GDPR).

[54] "Overview of EU General Data Protection Regulation," p. 5, Robbie Downing, 2017; As of October 2017, the UK's proposed Data Protection Bill, as it currently stands, exercises a number of permitted derogations from the GDPR.

[55] If yes, further consideration is needed. We can only process these categories of personal data in certain circumstances, including where the data subject has given explicit consent to the processing.

[56] "Overview of EU General Data Protection Regulation," p. 15-16, Robbie Downing, 2017; If yes, further consideration is needed. We can only process the personal data in certain circumstances.

[57] Article 5(1)(a), GDPR; 'lawfulness, fairness and transparency'.

[58] Article 5(1)(b), GDPR; 'purpose limitation'.

[59] Article 5(1)(c), GDPR; 'data minimisation'.

[60] Article 5(1)(d), GDPR; 'accuracy'.

[61] Article 5(1)(d), GDPR; 'accuracy'.

[62] Article 5(1)(e), GDPR; 'storage limitation'.

[63] Article 22, GDPR; See Article 4(4), GDPR, for definition of "profiling"; "Overview of EU General Data Protection Regulation," p. 26, Robbie Downing, 2017.

[64] Data protection issues should be immediately considered and not left until the end of a project.

[65] This might include features such as encryption or pseudonymisation, which would involve replacing an identifying feature of personal data such as a name with another artificial identifier so specific data subjects cannot be identified without knowing further information.

[66] Article 5(1)(f), GPDR; 'integrity and confidentiality'.

[67] "Overview of EU General Data Protection Regulation," p. 11, Robbie Downing, 2017.

[68] Articles 13-14, GDPR.

[69] Article 16, GDPR; "Overview of EU General Data Protection Regulation," p. 21, Robbie Downing, 2017.

[70] Article 15, GDPR.

[71] We should provide names of companies, not just broad categories such as "IT support companies."

[72] If we cannot set out an exact period, we need to set out how the period can be calculated.

[73] For example, this would be in connection with a contractual requirement if data subjects need to provide their personal data to register to use our IoT technology. Per a contract, data subjects might not be permitted to use our IoT technology otherwise.

[74] "Overview of EU General Data Protection Regulation," p. 12, Robbie Downing, 2017.

[75] "Overview of EU General Data Protection Regulation," p. 12, Robbie Downing, 2017.

[76] Detailed guidance on asking for, recording and managing consent provided by the Information Commissioner's Officer (ICO) in "Consultation: GDPR consent guidance," March 2017.

[77] See also Appendix A: Overview of Consent per the General Data Protection Regulation (GDPR).

[78] Article 7(1), GDPR; See also Article 4(11), GDPR, for definition of "consent."

[79] "In legal terms 'explicit consent' is understood as having the same meaning as express consent. It encompasses all situations where data subjects are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data." (WP29, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf)

[80] See Article 4(11), GDPR, for definition of "consent."

[81] If no, consent may not be valid.

[82] Article 7(3), GDPR.

[83] See WP29 for possible further guidance.

[84] Article 8, GDPR.

[85] Article 5(1), GDPR.

[86] "Overview of EU General Data Protection Regulation," p. 20, Robbie Downing, 2017.

[87] Articles 24-39, GDPR.

[88] Articles 27-33 & 37-39, GDPR.

[89] Articles 44-50 and Recitals 103-114, 117-119 & 167-169, GDPR; "Overview of EU General Data Protection Regulation," p. 35, Robbie Downing, 2017.

[90] We cannot transfer personal data outside the EU unless we have adequate safeguards in place such as a contract incorporating the appropriate version of the European Commission's Standard Contractual Clauses (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

[91] Article 33, GDPR.

[92] Article 34, GDPR.

[93] Articles 58, 83, 60-76 & 77-79, GDPR; See WP29 guidelines on guidelines on administrative fines.

[94] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[95] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[96] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications; Note that the ePrivacy Regulation amends the Privacy and Electronic Communications Directive (Directive 2002/58/EC).

[97] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG.

[98] http://eur-lex.europa.eu/eli/dir/2016/681/oj.

[99] "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 23, Article 29 Data Protection Working Party, adopted 16 September 2014.

[100] "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 24, Article 29 Data Protection Working Party, adopted 16 September 2014.

101 http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Data%20Mapping%20under%20the%20GDPR%20and%20Beyond.pdf.

102 "Building a European Data Economy," pp. 10-11,13, European Commission Staff Working Document, 10 January 2017.

103 "Building a European Data Economy," p. 9, European Commission Staff Working Document, 10 January 2017.

104 "Advancing the Internet of Things in Europe," p. 29, European Commission Staff Working Document, 19 April 2016.

105 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 7, Article 29 Data Protection Working Party, adopted 16 September 2014.

106 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 23, Article 29 Data Protection Working Party, adopted 16 September 2014.

107 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 23, Article 29 Data Protection Working Party, adopted 16 September 2014.

108 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 24, Article 29 Data Protection Working Party, adopted 16 September 2014.

109 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 24, Article 29 Data Protection Working Party, adopted 16 September 2014.

110 "Building a European Data Economy," p. 4, European Commission Staff Working Document, 10 January 2017.

111 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 6, Article 29 Data Protection Working Party, adopted 16 September 2014.

112 "Advancing the Internet of Things in Europe," pp. 22-23, European Commission Staff Working Document, 19 April 2016.

113 "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy," p. 45, European Commission Staff Working Document, 10 January 2017.

114 It is interesting to note that there is currently some ambiguity in the law concerning IoT systems and whether or not an error in a data transmission would be governed by product safety and product liability regimes. While providing data through an IoT system is considered a service, an erroneous data transmission may be caused by a product malfunction, which could lead to liability under product safety and product liability regimes.

115 "Advancing the Internet of Things in Europe," pp. 22-23, European Commission Staff Working Document, 19 April 2016; "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy," p. 41, European Commission Staff Working Document, 10 January 2017.

116 "Advancing the Internet of Things in Europe," pp. 22-23, European Commission Staff Working Document, 19 April 2016.

117 "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 13, Norton Rose Fulbright, February 2016.

118 "Advancing the Internet of Things in Europe," pp. 22-23, European Commission Staff Working Document, 19 April 2016.

119 "Advancing the Internet of Things in Europe," pp. 22-23, European Commission Staff Working Document, 19 April 2016; "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy," p. 42, European Commission Staff Working Document, 10 January 2017.

120 "Advancing the Internet of Things in Europe," p. 22-23, European Commission Staff Working Document, 19 April 2016; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

121 https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en.

122 http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en.

123 http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en.

[124] Presentation titled "The evaluation of the Product Liability Directive (85/374/EEC)," delivered by Hans Ingels during an EU workshop on liability in the area of autonomous systems and advanced robots and Internet of Things systems, 7 July 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-30/hans_ingels_-_the_evaluation_of_the_product_liability_directive_62081123-0251-9FA1-AD58076EF15FAB7D_46142.pdf. (Hans Ingels stated that the evaluation of the Product Liability Directive should be finalised by the end of 2017. This evaluation will assess: (1) "the overall functioning and the performance of the Directive;" (2) "whether it is effective, efficient, coherent and relevant;" (3) "EU added value in achieving its objectives;" (4) "the definition of product (e.g. to ensure it covers components (tangibles and intangibles) of the IoT);" (5) "the allocation of liability (ease of connected objects via IoT);" and (6) "the definition of defect (e.g. whether an unintended autonomous behaviour of an advanced robot could be considered as a defect).")

Presentation titled "EU product safety framework for advanced robots & autonomous systems," delivered by Felicia Stoica during an EU workshop on liability in the area of autonomous systems and advanced robots and Internet of Things systems, 7 July 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-30/felicia_stoica_-_the_existing_eu_safety_framework_with_regard_to_autonomous_systems_and_advanced_robots__iot-systems_6210B836-9707-D592-D33613EE1C6F086A_46145.pdf. (Felicia Stoica stated that the evaluation of the Machinery Directive should be finalised by Q1 2018. This evaluation will assess: (1) "Psychological aspects of human-machine collaboration," and (2) "Classification of applications in robotics (possible new standardization request).")

[125] Radio Equipment Directive 2014/53/EU, Article 3(3)

[126] Presentation titled "EU product safety framework for advanced robots & autonomous systems," delivered by Felicia Stoica during an EU workshop on liability in the area of autonomous systems and advanced robots and Internet of Things systems, 7 July 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-30/felicia_stoica_-_the_existing_eu_safety_framework_with_regard_to_autonomous_systems_and_advanced_robots__iot-systems_6210B836-9707-D592-D33613EE1C6F086A_46145.pdf.

[127] The Machinery Directive safety standards for robots are based or adapted on ISO standards, including those listed herein. (Presentation titled "EU product safety framework for advanced robots & autonomous systems," delivered by Felicia Stoica during an EU workshop on liability in the area of autonomous systems and advanced robots and Internet of Things systems, 7 July 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-30/felicia_stoica_-_the_existing_eu_safety_framework_with_regard_to_autonomous_systems_and_advanced_robots__iot-systems_6210B836-9707-D592-D33613EE1C6F086A_46145.pdf.)

[128] https://www.iso.org/standard/51528.html.

[129] https://www.iso.org/standard/51330.html.

[130] https://www.iso.org/standard/41571.html.

[131] https://www.iso.org/obp/ui/#iso:std:iso:13849:-1:ed-3:v1:en.

[132] https://www.iso.org/standard/53820.html.

[133] "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", Norton Rose Fulbright, February 2016.

[134] The Advisory Group to the European Community's Information Society Technology Program (ISTAG) has defined "ambient intelligence" (AmI) as "the convergence of ubiquitous computing, ubiquitous communication, and interfaces adapting to the user" (Gupta, M. (2003) "Ambient Intelligence - unobtrusive technology for the information society," *Pressbox.co.uk*, June 2017). In other words, a device that is AmI is sensitive and responsive to the presence of people.

[135] "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 4, Norton Rose Fulbright, February 2016.

[136] "Artificial intelligence & ethics," p. 1, Norton Rose Fulbright, 19 August 2017.

[137] "Building a European Data Economy," p. 4, European Commission Staff Working Document, 10 January 2017.

[138] "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy," p. 43, European Commission Staff Working Document, 10 January 2017.

[139] "Building a European Data Economy," p. 14, European Commission Staff Working Document, 10 January 2017.

140 http://ec.europa.eu/consumers/consumers_safety/product_safety_legislation/general_product_safety_directive/index_en.htm.

In the UK, the GPSD is implemented by the General Product Safety Regulations 2005 (GPSR) and the PLD is implemented by the Consumer Protection Act 1987 (CPA).

141 Specifically, how likely is our IoT technology to collect false negative or false positive data? ("Opinion 8/2014 on the Recent Developments on the Internet of Things," Article 29 Data Protection Working Party, p. 5, adopted on 16 September 2014.)

142 "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 14, Norton Rose Fulbright, February 2016.

143 "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 14, Norton Rose Fulbright, February 2016.

144 "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 18, Norton Rose Fulbright, February 2016.

145 This is especially important with life-sustaining IoT technologies.

146 "White hat" hackers are non-malicious hackers who test the security of companies' information systems.

147 "Building a European Data Economy," p. 13-14, European Commission Staff Working Document, 10 January 2017.

148 Recommendation: Every 6-12 months

149 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 22, Article 29 Data Protection Working Party, adopted 16 September 2014.

150 Per the UK's GPSD or the GPSR, we may have obligations to implement measures that enable us to be informed of risks posed by our IoT technology already on the market and to take appropriate action in response to such risks. That action may be a withdrawal from the market, adequately and effectively warning users, or a recall.

151 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 23, Article 29 Data Protection Working Party, adopted 16 September 2014.

Per the Product Liability Directive 85/374/EEC, cited in "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy," p. 40, European Commission Staff Working Document, 10 January 2017.

152 "Big Data and the Internet of Things, Protecting rights, controlling use and extracting value", p. 14, Norton Rose Fulbright, February 2016.

153 Detailed guidance on asking for, recording and managing consent provided by the Information Commissioner's Officer (ICO) in "Consultation: GDPR consent guidance," March 2017, https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

154 "Opinion 8/2014 on the Recent Developments on the Internet of Things," p. 22, Article 29 Data Protection Working Party, adopted 16 September 2014.

155 Good practices found in "Cyber security for Smart Cities: An architecture model for public transport," pp. 33-37, European Union Agency for Network and Information Security (ENISA), December 2015, https://www.enisa.europa.eu/publications/smart-cities-architecture-model.

156 Please note that "[m]ultiple thresholds can be set," and "[i]t is important to properly integrate dependencies to avoid cascade effect;" Good practices found in "Cyber security for Smart Cities: An architecture model for public transport," p. 36, European Union Agency for Network and Information Security (ENISA), December 2015, https://www.enisa.europa.eu/publications/smart-cities-architecture-model.

157 For example, "having alternate power sources available to run critical systems in the event of a power failure in the primary delivery system."

158 Articles 28 & 32-36, GDPR; "Overview of EU General Data Protection Regulation," p. 27, Robbie Downing, 2017.

159 Articles 37-39 & 83 and Recital 97; See WP29 guidelines on DPO; "Overview of EU General Data Protection Regulation," p. 28, Robbie Downing, 2017.

160 Article 30, GDPR.

161 Recitals 75-77, GDPR.

162 Article 35, GDPR; See WP29 guidelines on DPIAs; "Overview of EU General Data Protection Regulation," p. 31, Robbie Downing, 2017.

163 Article 25, GDPR; "Overview of EU General Data Protection Regulation," p. 32, Robbie Downing, 2017.

164 Not required by the GDPR; Articles 40-43 and Recitals 98-100, 148, 150 & 151, GDPR.

165 Not required by the GDPR; Articles 40-43 and Recitals 98-100, 148, 150 & 151, GDPR.

166 Article 32, GDPR.

167 Articles 33-34, GDPR; See WP29 guidelines on breach notification systems; "Overview of EU General Data Protection Regulation," p. 34, Robbie Downing, 2017.

168 Article 16, GDPR; "Overview of EU General Data Protection Regulation," p. 21, Robbie Downing, 2017.

169 https://ico.org.uk/.

170 Data subjects can request copies of personal data we hold about them and other information about the processing we carry out. See Article 15(1), GPDR.

171 Article 16, GDPR; "Overview of EU General Data Protection Regulation," p. 21, Robbie Downing, 2017; Per Article 19, if we have transferred the personal data to a third party, we need to notify them about the request from the data subject.

172 Article 19, GDPR.

173 Some circumstances in which we may be required to delete data subjects' personal data include the following. (1) It is no longer necessary for us to process the personal data for the original reason we collected it (e.g., if the data subjects no longer use our IoT technology). (2) We asked for data subjects' consent to process their personal data and they have withdrawn their consent. (3) If data subjects have objected to our processing and we do not have a strong business reason to carry on processing the personal data. (4) If there is a legal reason why we need to delete the personal data. (5) If we never had a lawful reason to process personal data originally.

174 Per Article 19, if we have transferred the personal data to a third party, we need to notify them about the request from the data subject.

175 Article 18, GDPR; "Overview of EU General Data Protection Regulation," p. 23, Robbie Downing, 2017.

176 Some circumstances in which we may be required to pause the processing of data subjects' personal data include the following. (1) To allow us to check the accuracy of the personal data. (2) If we never had a lawful reason to process personal data originally but data subjects do not want us to delete their personal data. (3) If we do not need the personal data anymore, but we need to keep them for a certain period of time for legal reasons. (4) If data subjects have objected to our processing of personal data and we are checking whether we have a really strong business need to carry on the processing anyway.

177 Per Article 19, if we have transferred the personal data to a third party, we need to notify them about the request from the data subject.

178 Article 20, GDPR; See also Article 12, GDPR; "Overview of EU General Data Protection Regulation," p. 24, Robbie Downing, 2017.

179 An example would be if data subjects are moving to use a competitor's IoT technology and need to provide information similar to the information they provided to us to operate the new IoT technology.

180 Articles 21-22, GDPR; See Article 4(4), GDPR, for definition of "profiling." "Overview of EU General Data Protection Regulation," pp. 25-26, Robbie Downing, 2017.

181 This would be a really strong business reason.

182 This might also be called an "opt-out."

183 "Advancing the Internet of Things in Europe," pp. 19-20, European Commission Staff Working Document, 19 April 2016.

184 Are we aware of the risks to proprietary software caused by open source licences?

185 "Building a European Data Economy," p. 10, European Commission Staff Working Document, 10 January 2017. Per the article, "[r]aw-machine-generated data are not protected by existing intellectual property rights since they are deemed not to be the result of an intellectual effort and/or have any degree of originality."

186 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943; “Building a European Data Economy,” p. 10, European Commission Staff Working Document, 10 January 2017. Per the article, for data to qualify as a “trade secret,” “measures have to be taken to protect the secrecy of information, which represents the ‘intellectual capital of the company.’”

187 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009; “Building a European Data Economy,” p. 10, European Commission Staff Working Document, 10 January 2017. Per the article, we must be a maker of a database, and the creation of such a database must “involve[] substantial investment in the obtaining, verfication or presentation of its contents.” If so, we may be granted “the right to prevent extraction and/or reutilisation of the whole or of a substantial part of the contents of [our] database.”

188 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029; “Too Much Information: How big data is changing legal and commercial risk management,” p. 3, Norton Rose Fulbright, September 2015.