Intelligent Campus:

Data Protection Impact Assessment

Draft 0-27 06/03/20

What's the Challenge?

Different "Intelligent Campus" systems could offer a wide range of benefits, from direct assistance to students (e.g. navigation apps) to economic and governance benefits to universities and third parties. To do this a wide range of data sources and processing may be considered, from room temperature and CO_2 level to face recognition and relationship mapping. Clearly some of these data sources are more intrusive than others.

Since data are often gathered from campus infrastructures (both physical and digital) that staff, students and visitors need to use for their education and research purposes, their support for this data gathering and use is essential. If campus occupants perceive intelligent campus applications as threatening, intrusive, or just creepy, they are likely to change their behaviour. While they may intend only to frustrate the gathering or use of data that they consider unacceptable, such changes are also likely to damage the infrastructures' main purpose of supporting teaching and research. For example if they feel they are being "tracked" students may avoid monitored physical spaces such as lecture theatres or routinely swap access cards or passwords to obscure their traces; staff and students may use unofficial cloud services ("shadow IT") rather than those provided by the institution, or connect to mobile phone data rather than the campus wifi network.

At an early stage of the design of any intelligent campus application, the following questions need to be considered:

a) Is the proposed use of sensors/data likely to be perceived as intrusive?
b) What safeguards can be applied to demonstrate safety and benefit?
c) Will campus users consider that the benefits of the proposal justify its impact?

Privacy Impact Assessments (PIA) are a tool designed to answer these and similar questions. These were advisory, rather than a requirement, under the European Data Protection Directive, but have now been formalised (as "Data Protection Impact Assessments" (DPIAs), with regulators using the terms interchangeably) under the General Data Protection Regulation (GDPR). The GDPR requires a full DPIA for some types of high-risk processing (see Box 1), but the approach is also useful at lower levels of privacy/data protection intrusion.

In particular, the Article 29 Working Party of Data Protection Regulators **approved** a **PIA toolkit for Radio-Frequency ID (RFID) tags** in 2011 (referred to hereafter as the "RFID Toolkit"). Since some intelligent campus systems already use RFID tags, and many others have similar characteristics, that toolkit appears a good basis for assessing the privacy/data protection impact of intelligent campus systems. Specifically, the RFID toolkit proposes a four-point scale to determine whether, and how intense, a DPIA is required; it then suggests lists of both risks and mitigation measures that should be considered. As described in a paper in the Journal of Information Rights, Policy and Practice – "**See No…, Hear No…, Track No…: Ethics and the Intelligent Campus**" – this Intelligent Campus DPIA toolkit generalises and extends that approach.

How can a DPIA help?

A Data Protection Impact Assessment shares many of the characteristics of a traditional risk assessment: in particular the need to identify risks, assess their severity, identify measures that can be used to manage them, and agree which of those measures will be adopted. However in a DPIA the risks considered are those to privacy and data protection, and the perspective taken is that of the individual whose data are processed, not that of the organisation.

Thus, for example, an information security breach might appear on a business risk assessment as a regulatory, operational and financial risk: in a DPIA it must be considered as creating a risk of harm to the individuals whose data may be accessed, modified, or destroyed.

Most DPIA processes involve two stages:

- first an initial analysis to determine whether a DPIA is required and, if so, whether that should be small-scale or full (under the GDPR, some of the latter may be mandatory and have to meet specific legal requirements – See Box 1);
- then, if required, the appropriate DPIA itself.

For Intelligent Campus applications, this toolkit uses a five-point scale for assessing risk, based on distinctions made in laws, cases and regulatory guidance:

0) **Presence**: data that is not about individuals;
1) **Counting**: the number of individuals in a place or route;
2) **Identifying**: individuals and/or linking to other data sources;
3) **Recording**: so that past data can later be reprocessed;
4) **Analysing**: data continually, e.g. face-recognition or relationship mapping.

Level 0 applications should not require a DPIA, level 1 should be subject to a small-scale DPIA, levels 2 and higher to a full DPIA.

Having decided to conduct a DPIA, this toolkit provides suggestions for both: the kinds of risks to individuals that are likely to arise in Intelligent Campus applications and should be considered in their DPIAs; and the kinds of controls that can be used to manage those risks. Once the organisation has assessed the risks and chosen appropriate controls, it can determine whether the remaining risk is likely to be acceptable to those who use the campus spaces and infrastructures.

Under the GDPR, there is strong encouragement to involve stakeholders – in particular those whose data will be processed – in this assessment. Which risks are they concerned about? Which controls would they consider reasonable? Are they comfortable with the remaining risk?

Mandatory DPIAs

The European Data Protection Board (EDPB) has endorsed the following list of characteristics likely to indicate high-risk processing.

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive or highly personal data
- Large-scale processing
- Matching or combining datasets
- Vulnerable data subjects
- Innovative use/new technical or organisational solutions
- Processing prevents data subjects from exercising a right or using a service or contract

Any processing involving two or more of these is likely to require a DPIA that satisfies the process and documentation requirements of GDPR Article 35.

The Information Commissioner has **detailed guidance on when a DPIA will be mandatory**, including on how this applies to innovative technologies.

Box 1 Mandatory DPIAs

Thus the DPIA process offers a structured way to answer the most important question about an Intelligent Campus deployment: will it be acceptable to those who use the campus, or will it be perceived as objectionable to their normal use of campus infrastructures? Identifying unacceptable proposals, and improving acceptable ones, early in the life of a project can save large amounts of wasted or even counter-productive cost and effort.

Conducting a DPIA

Many documents already describe processes for conducting DPIAs. For most Intelligent Campus applications, the most relevant may be the **Article 29 RFID Toolkit** and **UCISA's PIA Toolkit**; for high risk applications, where a DPIA is mandatory under the GDPR and specific documentation requirements apply, it may be useful to follow a process designed by Data Protection Regulators, for example the **UK Information Commissioner** or the **Article 29 Working Party's general approach**, recently **endorsed** by the European Data Protection Board (EDPB). The table indicates the stage in each DPIA process where the following Appendices should be used:

	Art.29 RFID Toolkit	**UCISA PIA Toolkit**	**ICO How do we do a DPIA**?	**Art.29 General Approach**
App.1	2.1 Initial Analysis	2.1 Identify need for a (D)PIA	Step 1 How to decide whether to do a DPIA	III.B.a processing likely to result in a high risk
App.2	2.2 Step 2 (replaces Annex III)	2.3 Identify privacy and related risks	Step 5 How to identify and assess risks	III.D.c what is the methodology
App.3	2.2 Step 3 (replaces Annex IV)	2.4 Identify and evaluate privacy solutions	Step 6 How to identify mitigating measures	III.D.c what is the methodology

Whichever model is chosen, a DPIA begins by identifying the data and dataflows that are involved in an application. This information should be sufficient to conduct the Initial Analysis: Appendix 1 to this document (based on the RFID Toolkit) sets out the likely risk levels for Intelligent Campus applications.

If the Initial Assessment concludes that a DPIA is required then the organisation should document the data and flows in detail, including the purpose and benefits, the legal basis/bases for processing and the status (data controller or data processor) of the organisations involved. Forms for recording this information are contained in each of the DPIA process documents identified above – for example Annex I of the RFID Toolkit.

The organisation should then identify the privacy and data protection risks that the data and processing may cause to individuals. Appendix 2 to this document (based on Annex III of the RFID Toolkit) suggests the risks that should be considered.

The organisation should then identify the controls that can be used to reduce and manage those risks. Appendix 3 to this document (based on Annex IV of the RFID Toolkit) contains suggestions.

The organisation can then determine whether the risks can be managed to an acceptable level, given the benefits that the processing will deliver. This conclusion should be documented and, if the proposal is acceptable, the controls transferred into the project plan.

Appendix 1 – Intelligent Campus Risk Levels

Risk Level	Definition
0	**Presence**: whether a space is occupied, including whether the number of occupants is small or large. This could include, for example, sensing the number of wireless connection requests, the sound level, or motion detection. No identifiable information is processed, even to derive occupancy.
1	**Counting**: referred to as "statistical counting" in the draft ePrivacy Regulation. The canonical example is measuring queuing time by calculating how long wireless devices are stationary before moving past a bottleneck. This requires monitoring the location of individual devices over a short time period, as part of the calculation. However there is no need to link the device identifiers to their users, to any other information source, or to the desired output. Safeguards should be built in to prevent such linking.
2	**Identifying**: including "singling out" in the **Article 29 Working Party guidance**. These applications gather sense data in forms that either will be, or could be, associated with an individual, either to further link to other information sources such as their name or subject, or to provide personalised service to that individual. Human-monitored CCTV and mobile apps that are aware of their current location are examples that will generally fall into this category.
3	**Recording**: systems that record sense data for occasional later processing, for example recording of CCTV in case it is subsequently needed to investigate an incident.
4	**Analysing**: systems that involve continuous processing of sense data, such as face recognition, audio analysis for trigger words, or tracking of behaviour or relationships between individuals. The identification of face recognition as a biometric by both the **European Data Protection Supervisor** and **Information Commissioner** means that at least some of these applications will need to be treated as involving Special Category Data.

An intelligent campus can typically detect humans using three 'senses': video, audio and location. Common examples of video are CCTV and motion sensors; audio is less common, but microphones are used to monitor noise levels and may be included in some CCTV systems; location often involves mobile devices – either by external observation of their Bluetooth, WiFi or mobile phone transmissions or by devices determining their own location using sensors such as GPS – but also fingerprint readers, swipe and payment cards that are presented at particular, known, locations such as doors or shops.

While it is tempting to rank these senses by intrusiveness, as the following table shows, all three can in fact be used in both intrusive and unintrusive ways. Vision can be used to sense whether a room is full or empty, or to track individuals using face recognition; hearing can be used to measure activity in a space, or to record conversations and recognise individuals; location can provide approximate headcounts, or track an individual and their contacts throughout the day and night. Thus, when assessing the risk from an intelligent campus application, the characteristics of the application, rather than the particular sense used, are likely to be more important. It may, however, be helpful to consider the choice of sense as a possible control measure: for example video is more likely to respect opaque boundaries such as walls. Considering sensor choice as a mitigation measure, rather than as the main determinant of risk, highlights the suitability of novel sensors such as CO_2 level for low-risk applications.

Risk Level	Video	Audio	Location
0. Presence	Motion sensor	Sound level	Wifi/Bluetooth activity
1. Counting			Wifi/Bluetooth queue monitors
2. Identifying	Monitored CCTV		Location-aware app
3. Recording	Video recording	Audio recording	Logfiles/Access Cards
4. Analysing	Automatic Number Plate Recognition (ANPR)/Face recognition	Voice recognition/trigger words	Relationship mapping

Appendix 2 – Intelligent Campus Risks

Whichever Data Protection Impact Assessment process is chosen, it is likely to require the organisation to consider what risks may arise to individuals, and then to ensure that those risks are managed and maintained at an acceptable level. This Appendix identifies the risks most likely to arise in intelligent campus applications: Appendix 3 below suggests the kinds of measures that are likely to be used to manage them.

Note that the aim of a DPIA is to understand risks and how they can be managed, not to eliminate them all.

Privacy Risk	Description and Examples
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. **Example**: No documentation of purposes for which intelligent campus systems used and/or use of intelligent campus data for unlimited range of analyses.
Collection exceeding purpose	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. **Example**: Desk occupancy system collects identities of users, rather than just whether desk is free/busy.
Incomplete information or lack of transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. NB this is a particular challenge where data are collected by observation, rather than direct interaction with the individual. **Example**: Information available to staff/students/visitors lacks clear information on how intelligent campus data is processed and used, the identity of the Operator, or the user's rights.
Combination exceeding purpose	Personal data is combined to a greater extent than is necessary to fulfil the specified purpose. **Example**: Wifi queue-monitoring information is combined with login records to determine location of individuals.
Multiple, incompatible purposes	Personal data is used for multiple purposes that are neither compatible nor provided as separate options to individuals. **Example**: Swipe card data is not only used to unlock doors, but to build study profiles of students. **Example**: CCTV systems installed for campus security are re-used to monitor lecture attendance.
Loss of practical obscurity	Tracking spilling into private space; private (inter)actions being captured by public sensors. **Example**: Every student in college accommodation is tracked 24x7 through wifi usage.
Sensitive or high-risk data	Unplanned capture of data that are either sensitive or otherwise represent a high-risk to individuals or the organisation. **Example**: Location data in counselling/medical service can reveal identities (and possibly problems, by linking to clinic timetables) of those who have been seeking help. **Example**: Video/audio of meeting rooms may capture confidential discussions/presentations.

	Example: Location data in accommodation may identify overnight visitors.
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose. **Example**: Personal data is collected by an intelligent campus system and is saved for an indefinite period.
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage. **Example**: Use of campus app requires accepting advertising cookies
Secret data collection by intelligent campus operator	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. **Example**: Information is collected while individuals walk across campus and no notice warns them about intelligent campus sensors
Inability to grant access and other rights	There is no way for data subjects to initiate a correction or erasure of their data. **Example**: Operator cannot give student a full picture of what is saved about him or her as a result of being present on campus.
Prevention of objections	There are no technical or operational means to allow complying with a data subject's objection. **Example**: At-risk student cannot opt out of video/audio observation while on campus.
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decision making. **Example**: Navigation app sends users who walk faster via longer routes to reduce congestion
Paternalism or discrimination by algorithms	Algorithms make decisions that are discriminatory, or should be left to the individual. **Example**: Navigation app sends user by a longer route because health data shows they should be taking more exercise
Algorithms unaware of context	Algorithms apply 'one size fits all' rules without awareness of external/invisible circumstances. **Example**: Algorithm calculates that student is at risk of dropping out when, in fact, they are learning from paper books rather than online.
Decisions based on poor-quality data	Decisions are made that do not take account of the likely (in)accuracy of the source data. **Example**: System concludes from swipe-card data that a building is empty, when staff routinely hold doors open for one another.
Insufficient data/system security	Security mechanisms to protect data, systems and sensors do not provide appropriate protection for the sensitivity of data or processing. **Example**: Software vulnerability lets intruders access CCTV cameras.

	Example: IoT device does not implement strong encryption, allowing information to be seen by others. **Example**: Inadequate access controls allow members of staff to see the Principal's current location.
Deanonymisation/De-pseudonymisation	Data that is supposed to be anonymous/pseudonymous can be associated with individuals, whether using patterns, combinations of datasets or external information. **Example**: Anonymous data recorded in a student bedroom is likely to relate to its occupant. **Example**: Desk occupancy information combined with login information from network socket can reveal individual's working habits.
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation, etc. **Example**: Intelligent Campus Operator shares collected information with a third party without consent or other legal basis
Insufficient logging mechanism	The implemented logging mechanism is insufficient. **Example**: No logs of who has accessed the intelligent campus data.
Uncontrollable data gathering by intelligent campus sensors	Intelligent campus systems collect data about people who are neither staff nor students. **Example**: Wifi sensors track all those on, or near, campus
Reduced participation	Intrusive use of sensors/data causes individuals to avoid using services. **Example**: University's use of Wifi location data to profile students' study habits causes students to stop using eduroam and location-aware apps
Perceived surveillance causes individuals to change behaviour	Individuals who feel they are under surveillance may change what they say or do, potentially harming their rights to free speech & free assembly. **Example**: Concern about 'surveillance' by CCTV causes staff to avoid sensitive topics in lectures.

Appendix 3 – Intelligent Campus Controls

This Appendix suggests the kinds of measures that are likely to be used to manage the risks to individuals arising out of intelligent campus applications.

Control Measure	Description and Examples
Application Governing Practices Measures to ensure that organisations choose appropriate uses of intelligent campus technology, and design, implement and operate them safely.	Governing the **choice** of Intelligent Campus applications: • Policies on the definition and assessment of purposes, including Data Protection Impact Assessments where appropriate; • Provisions to determine the compatibility of different purposes, and to offer granular choices to individuals; • Policies on the choice of sensors/data, especially where existing sensors/data are re-purposed; • Policies covering high-risk locations (e.g. residences, counselling services): whether intelligent campus technology is appropriate and if data require special treatment (e.g. reduced location precision, stronger access control); • Policies governing any data sharing (e.g. with commercial partners); • Provisions in place to deal with concerns or behaviour change among those who use monitored spaces. Governing the **design and conduct** of Intelligent Campus systems: • Management practices by the Intelligent Campus system operator; • Policies related to lawful processing of personal information; • Privacy by Design provisions, including minimisation of data collection and processing (including use of anonyms/pseudonyms), default settings (where appropriate); • Retention, disposal and erasure policies for intelligent campus data; • Policies to address processing or storing of information about visitors and guests, as well as staff and students; • Governance of algorithms (relating to discrimination, paternalism, data quality, etc); • Security Governance practices.
Providing Individual Access and Control Measures to provide individuals with information about, and control of, data gathering and use	• Providing information about the purposes of the processing and the categories of personal data involved; • Clear process to object to the processing of personal data or grant/withdraw consent for different purposes; • Clear process to request rectification or erasure of incomplete or inaccurate personal data; • Providing technical controls where possible, e.g. location-aware apps that individuals can choose to install/enable/disable (e.g. at particular times or in particular places).
System Protection Measures to address the protection of personal data in communication infrastructures and back-end systems.	• Access controls related to the type of personal data and functionality of the systems are in place; • Audit and system logs related to the type of personal data, functionality of the systems, and actions of their operators are in place, as well as appropriate protection for those logs from intentional or unintentional harm;

Note that those systems may be sufficiently complex to justify a DPIA in their own right: at least the listed issues should be covered	• Controls and policies to ensure the Operator does not link personal data in the Intelligent Campus systems in a manner inconsistent with the DPIA Report (in particular to protect pseudonyms and anonyms);
	• Controls and policies to ensure those with access to systems and data are appropriately trained, supported and monitored;
	• Appropriate measures to protect the confidentiality, integrity, and availability of the personal data in the systems and in the communication infrastructure;
	• Policies on the retention and disposal of the personal data;
	• Policies and processes for incident detection, response and notification;
	• Implement information security controls, such as:
	  • Measures that address the security of networks and transport, storage and processing of Intelligent Campus data (e.g. encrypted communication with sensors);
	  • Measures that facilitate the availability of Intelligent Campus data through appropriate resilience, back-ups and recovery, and well as appropriate measures to protect the security of resilient systems and back-ups

Sensor, Device and App Protection Measures to address the protection of personal data in sensors, devices and apps. These should be in addition to any controls that may be available to the user (under Individual Access and Control above) to disable sensing or processing, either temporarily or permanently.	• Access control to information and functionality, including authentication of sensors, apps, and underlying processes, and authorisation (if appropriate) to communicate with the device/app; • Physical and logical security of sensors against unauthorised access/reconfiguration; • Measures to assure/address the confidentiality of the information (e.g. through encryption by device/app); • Measures to assure/address the integrity of the information; • Measures to secure any information retained after the initial collection (e.g., duration of retention, procedures for eliminating the data at the end of the retention period or for erasing the information in the device/app, procedures for selective retention or deletion of data); • Security of any app/programme/device itself; • Minimising the technical capability of sensors to only the functionality required (e.g. mobile app should not request access to phone functions it does not need; location-aware apps should stop tracking when not active; sound-level sensors should be disabled from acting as microphones).
Accountability Measures Measures to address procedural data protection, accountability and external awareness of intelligent campus applications.	Ensuring the easy availability of a comprehensive **information policy** that includes: • Identity and contact details of the Intelligent Campus Operator; • Purpose(s) of the Intelligent Campus Application; • Types of data processed by the Intelligent Campus Application, in particular if personal data are processed; • Type(s) of data source/sensor used and how these are protected against misuse; • Whether the locations of individuals, or their devices, will be monitored; • Information about any automated decision-making that may be used; • Likely privacy and data protection impacts, if any, relating to the Intelligent Campus Application and the measures available to mitigate these impacts; • Link to any DPIA that has been conducted

Ensuring concise, accurate and easy to understand **notices** of the presence of Intelligent Campus data collection/sensors that include (at least):

- The identity of the Intelligent Campus Application Operator;
- The purpose(s) for which data are being collected;
- Any third parties with whom the information will be shared;
- A point of contact for individuals to obtain the information policy.

Noting if and how **redress mechanisms** are made available:

- Intelligent Campus Operator accountable legal entity;
- Point(s) of contact of the designated person or office responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures related to the protection of personal data and privacy;
- Inquiry methods (e.g., methods through which the Intelligent Campus Application Operator may be reached to ask a question, make a request, file a complaint, or exercise a right);
- Methods to object to processing, to exercise access rights to personal data (including deleting and correcting personal data), to grant/revoke consent, or to change controls and other choices regarding the processing of personal data, if required or otherwise provided;
- Other redress methods, if required or otherwise provided.