

Land surveying is the process of establishing a property's features, physical characteristics, and boundary lines. It facilitates the preparation of a map or plan that encompasses everything from private properties and engineering features—like buildings, roads, and canals—to entire states and countries.

The significance of land surveying is observed in urban planning, real estate, construction, and infrastructure inspection. It requires the use of cutting-edge technologies like drone mapping, mobile mapping, satellites, and GPS systems.

These technologies are not designed to detect and exclude faces of humans, vehicle licence plates, and other data types that could be personal to individuals. Although not directly, a land survey may often include the collection of some data, which brings it under the scope of GDPR.

The importance of GDPR compliance in land surveying

[GDPR Article 4](#) draws the definition for personal data as "any information relating to an identified or identifiable natural person who can be identified, either directly or indirectly, in particular by reference to an identifier. Identifiers could range from name and identification number to location data or an online identifier."

Let's understand instances when data types could be personal. Respondents' submission of ideas on how to redevelop an urban area could be simply opinions instead of personal information. However, when asked to map their commute from home to work, the surveyor can get to know where an individual works and what their home address is. Such information eases the process of identifying the respondent and hence is classified as personal information.

Such personal data of individuals collected directly or indirectly poses a great risk to their privacy and security, even if it's deliberately not meant so. Data protection laws like GDPR mandate entities involved in data collection to respect the data privacy rights of individuals. It requires

them to process personal data responsibly, ensuring no room is allowed for data to be misused or exposed to unauthorised parties.

Surveyors need to be highly cautious with their data processing practices. They should ensure their data processing methods are carried out in adherence with principles and requirements stipulated under the GDPR regulations. Obtaining consent (Articles 6 & 7), purpose limitation (Article 5(1)(b)), data retention (Article 5(1)(e)), data minimisation (Article 5(1)(c)), and security of processing (Article 32) are pivotal to ensuring compliance with GDPR.

Violating these principles can result in two major consequences:

- Fine ([Article 83](#)): up to 20 million euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Compensation ([Article 82](#)): calculated on a case-per-case basis by the national data protection authority (NDPA).

Personal data collection in land surveying

Firstly, data collected in conducting a land survey includes up-to-date information on names and addresses of the property owners, which surveyors can collect through either accessing records from government land record offices or third-party data providers. Surveyors should be aware of the fact that such data, like names and addresses, are categorised as personal data under most data protection laws, including GDPR.

Secondly, one party involved in the land survey may be sharing project photos with third parties or subprocessors, including tax administration, execution authorities, trade organisations, financiers, and other external service providers for the processing of assignments.

These subprocessors could process this data either on behalf of the surveyor or for their own purposes. In most cases, as it is observed with the rise of AI, the processor could apply algorithmic tools to make

educated guesses about individuals. They may even combine this piece of data with other datasets to identify individuals who were part of the land survey in the first place, potentially compromising their privacy and security.

Thirdly, aerial photography of land as part of the survey may inadvertently capture visual media of people, vehicles, or buildings. Such data may potentially be used to identify individuals directly or indirectly. Let's understand this with data collected for a land survey as a subset of geospatial data. Geospatial data comprises many other forms of data in addition to land survey data, including aerial photographs, satellite imagery, demographic information, maps, and environmental data.

- When these aerial photographs are integrated into the geographic information systems (GIS)—a software tool for mapping and analysing geographic data—they are often mixed with other layers of data, including parcel boundaries and numbers. Some countries even maintain a public record of parcel numbers for people to find information about property ownership, which is usually made available by the county assessor's office. When aerial photography and parcel numbers are integrated in GIS platforms, it eases the way for people to look up ownership details of a property with the tagged parcel number.
- The other way through which details about property owners can be accessed is through cross-referencing aerial photographs and land survey records. Physical markers associated with a property include concrete monuments, iron pipes, or natural features registered in the records in reference to specific property. Location in terms of latitudes and longitudes of these markers can be determined using georeferencing techniques, e.g., GPS. High-resolution images can further be analysed to extract details, including rivers, roads, or buildings nearby, which further corroborate the marker's location.
- A land survey includes photography of not only bare land but also the land with existing structures, like homes. Aerial imagery or mobile mapping may capture specific features of structures, including building footprints, specific parking arrangements, surrounding vegetation, etc. When georeferenced and correlated with publicly available records or maps, it can potentially lead to their distinction or identification. This method affects the privacy of individuals in two ways: first, that the layouts of homes that a person wants to keep private are accessible publicly, and second,

that the georeferenced data, if regularly updated, gives rise to constant surveillance.

Fourthly, aerial photography, mobile mapping, or similar land surveying methods and technologies can capture excess data in addition to land features, including images of individuals in open spaces, bodies, and vehicle licence plates. These data make the most fundamental and highly visible elements of one's identity and can facilitate identification of individuals. While the faces of individuals make the direct case of identification, vehicle licence plates can be traced back to individuals and are, therefore, considered indirect identifiers.

Anonymisation as a solution for protecting personal data in photos

For this theme, we will focus on point number four, which is about how aerial photography in public places can capture individuals' personal data.

Obtaining explicit consent as a requirement for lawful large-scale data processing can be time- and resource-consuming, given millions of PII captured in aerial photos could be directly or indirectly linked to identifiable natural persons.

Fortunately, there are market-fit, technological solutions that allow surveyors to carry out their job while still protecting people's privacy. These solutions work as a saviour of all business models that involve large photo collections and processing large imagery datasets.

[GDPR Article 25](#) emphasises implementation of the privacy-by-design framework. It requires companies and organisations to implement technical and organisational measures at the earliest stages of the product/operation design. Anonymisation of data is a core principle of privacy by design. It removes personally identifiable information from images and videos.

Anonymisation renders PII unlikely to link back to specific individuals. [GDPR Recital 26](#) states that anonymised data are not considered personal information. Therefore, it has become the de facto measure for

processing personal information, as it also eliminates the need for consent.

The challenge in anonymisation is the detection of objects to be blurred. In principle, removal of as much information from images as possible is suggested, but faces and licence plates are mostly anonymised. When a [data subject access request](#) (DSAR) is made, it is the organisation's responsibility to anonymise the faces and licence plates of all but the subject so as not to breach the privacy rights of anyone else captured in the land surveying process.

Anonymisation software should have the ability to accurately detect identifiable elements and blur it in a way that anonymised objects can't be retraced back to individuals. Objects that, even after anonymisation, can be re-identified risk non-compliance with GDPR. Convolutional neural networks (CNNs), specific types of deep learning models, are used to detect grid-like data (structures and objects in images, such as faces).

Anonymisation methods to obscure individuals' identities:

- The blurring technique essentially blurs or pixel filters the facial regions of individuals to obscure their identity. Blurring de-emphasises personal information without completely obscuring it. It conceals facial regions or personally identifiable elements yet maintains the integrity and context of the image. When an image is blurred, viewers can figure out that blurred components are part of a larger picture.
- The masking method overlays a solid colour or an artificial mask on top of the face or a number plate to effectively anonymise it. Using the masking technique, PII can be de-identified and de-sensitised in such a way that it cannot be re-identified or recovered even with additional information. While in most contexts, masking is associated closely with pseudonymisation, its application in anonymisation is an irreversible process.

Protecting personal data in photos through GDPR compliance in land surveying

In this digital age, it is crucial to balance data utility and data privacy. With identity theft and data breaches making headlines, data privacy is unarguably the utmost concern of people. Land surveying can inadvertently capture personal information that may have implications for people's privacy.

Surveyors should be mindful of employing their technologies, like aerial photography and mobile mapping, to respect the privacy rights of individuals and ensure compliance with data protection laws. By employing techniques like photo anonymisation techniques that blur or mask face and licence plate effectively, land surveyors can achieve a compliance-friendly way to do their job while maintaining people's anonymity.