



GUIDANCE TO CUSTOMERS ON CAMERA INSTALLATION AND USE

This guidance provides important information about legal obligations you have as the operator of a camera system.

This guidance is not intended to provide a comprehensive explanation of applicable privacy laws, nor constitute legal advice.

If you have any concerns or questions about these matters, you should take legal advice and check advice published by your local data protection supervisory authority.

You may also wish to read the Guidelines prepared by the European Data Protection Board on processing personal data through video devices.

ARLO CAMERA SYSTEM

We have prepared this guidance to help you understand how to use your Arlo camera system in accordance with data protection laws. In this note “you” means you (our customer) and “we” and “us” means Arlo.



DATA PROTECTION LAWS

Data protection laws, such as the General Data Protection Regulation (GDPR), regulate the collection, use and processing of personal data.

These laws are designed to protect individuals' right to privacy. They put legal obligations on your operation of cameras, including positioning, notices (signage) required in the monitored space and the way in which data can be used and shared.

If you use the system within your private household, the data protection laws may not apply to you, as we describe further below.



INSTALLATION AND POSITIONING OF THE CAMERAS

The location and positioning of cameras is very important from a data protection perspective. This is because cameras may capture images which people may not expect to be recorded.

When setting up your cameras you should position them carefully and should look at how the camera settings can be used to avoid certain areas of view.

As the operator of the system, you are ultimately in control of the area being monitored by the cameras and access to it (and thus who may be monitored and recorded). You need to be comfortable with these responsibilities.



If you are installing cameras, some simple principles to bear in mind to ensure they are positioned lawfully are:

- i. only place cameras in areas where you are concerned about a safety or security risk (e.g. potentially vulnerable entrances, exits or windows);
- ii. limit the camera's field of view to areas within your property boundaries and avoid monitoring neighbouring premises. Some of the camera settings can help with this by allowing you to zoom in and fix on areas within the field of view
- iii. do not place cameras in areas where people would not reasonably expect images to be captured;
- iv. avoid locating cameras in areas where there may be sensitivity due to the nature of the space and personal activity taking place there e.g. in or near bedrooms, toilets, spa zones, changing areas or other sensitive spaces that people expect to be kept private;
- v. do not place cameras in areas which would provide a view of recreational public areas – for example public parks, public benches or outside café tables;
- vi. take particular care when placing cameras in any areas where there are children or vulnerable adults, because such people have additional protections under privacy laws;
- vii. if there are a number of occupiers of the site (e.g. it's a shared, communal space or building), you are responsible for getting permission to install the system from other owners / occupiers at the premises.



arlo 



“Hi, can you leave it
with our neighbour?”

AUDIO

Arlo cameras have a built-in microphone which, can capture audio from several metres away. Please take care to avoid breaching any relevant local laws on audio recording.

Some of the camera settings can help reducing the audio detection sensitivity, disable the audio detection or disable the microphone.



VIDEO DOORBELL CAMERAS

In addition, when (re)configuring or installing a video doorbell camera yourself, you should always seek to minimize coverage of public areas (e.g. street), common areas (eg shared property/ a lobby area) and another person's property (neighbour's garden, entrance or house) by:

- i. Using the angled mount, which is supplied and included in the box of video doorbell, to angle the camera's field of view;
- ii. adjusting the following camera settings (using the Arlo App & Web) so as to:
 - o crop the field of view;
 - adjust the field of view of the doorbell camera in the video settings;
 - adjust the camera's motion detection settings in order to avoid recording video when motion is detected in such areas.
 - create activity zones to focus motion detection on the specific areas within you property (subscription required for Cloud activity zones)



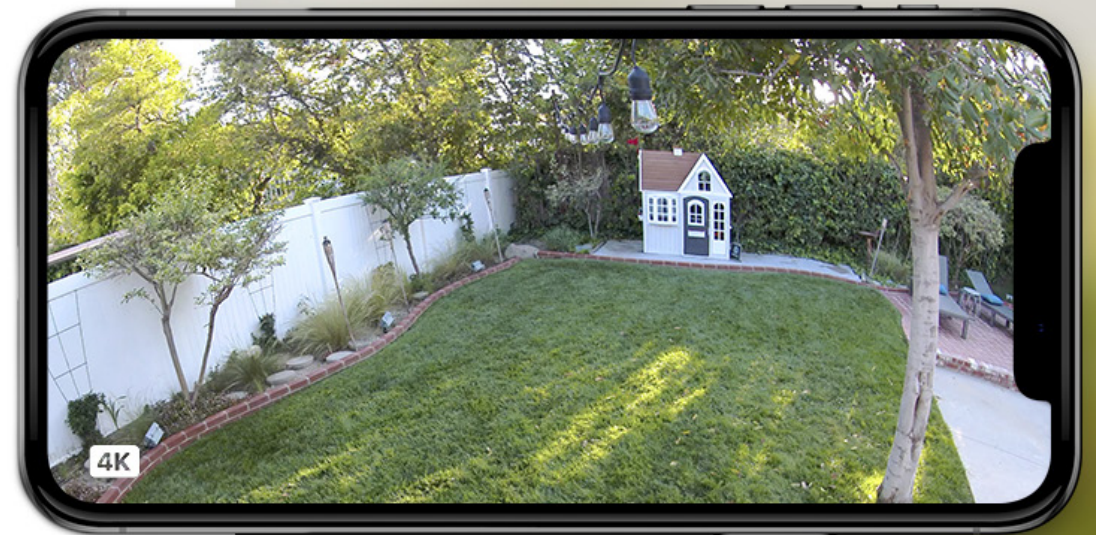
IF YOU ARE A HOUSEHOLD USER

If you install and use Arlo cameras solely within your private household, the GDPR is unlikely to apply to you. This is because the GDPR does not extend to data captured and used solely within the home setting. This is commonly known as the «household exemption.»

In this case, you won't have a legal obligation to comply with the responsibilities set out in this guidance note, although you should still use the cameras responsibly to protect the privacy of others.

Please note that the household exemption is limited; the GDPR rules may apply if you:

- monitor the activities of workers or domestic staff working within your household,
- capture images from outside your property,
- share images on social or other public media.



NOTICE / SIGNAGE

You must position warning notices/signs at the premises to help people understand that the area is being monitored.

Notices/signage should be placed in such a way as to be visible to people before they enter the monitored area.

They should include basic information to explain that a monitoring system is in place, that you are the operator of the system and the purposes for which you will use any data that is captured (e.g. security of the premises).

If you are using the system within the scope of the household exemption (described above), it is still advisable that you let members of the household and visitors know that you have cameras in operation at your home.

A window sticker that can be used to alert visitors to your camera can be found in every Arlo camera box. If you did not receive a sticker you can contact customer care for support.

[Please see for a template notice/sign that you may wish to use for these purposes.](#)



arlo 

VIEWING IMAGES FROM THE CAMERA SYSTEM

Arlo cameras include remote access controls that, depending on the camera type, allow you to capture and store images and/ or audio on your own devices (e.g. via our app).

It is important that you use these features selectively, where there is a genuine need to look back at the image – for example, where you are concerned that there has been a security incident at the premises which you would like to review or investigate further. You should not use these features to, for example, continuously monitor an individual or their behaviour at the premises.



arlo 

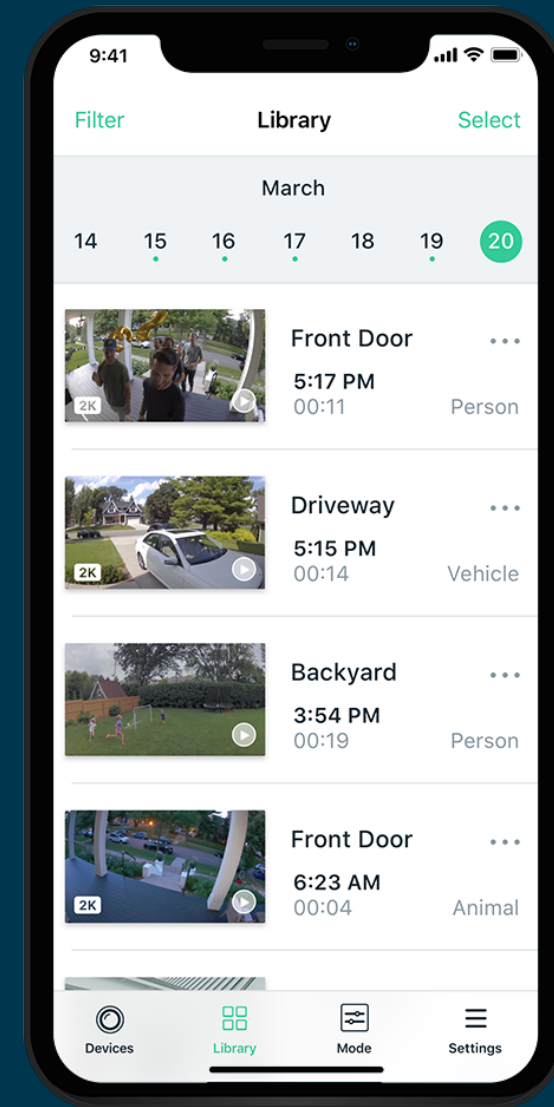
MANAGING IMAGES CAPTURED FROM THE CAMERA SYSTEM

You must take care regarding how you use and (if relevant) share any images captured by the Arlo cameras with other people.

You should only share images with others where you are comfortable that disclosure is necessary and appropriate and won't cause embarrassment or harm to anyone captured within the images.

Be particularly careful about sharing images in any public or semi-public environment, for example on the internet or social media.

We recommend that you do not post images on these platforms unless you have consent from each of the individuals within the images.



ADDITIONAL OBLIGATIONS IF YOU ARE A BUSINESS USER OR YOUR USE IS OUTSIDE THE <<HOUSEHOLD EXEMPTION>>

If you are a business user, or if you use the system outside the scope of the household exemption, you will need to comply with the legal responsibilities set out in the GDPR which apply to a 'controller' of personal data.

In these cases, it is important that you familiarise yourself with your legal responsibilities under the GDPR as failure to install and use the system properly could cause significant legal risk.

You may find it helpful to consult information provided by your local data protection supervisory authority regarding your responsibilities as a controller.



arlo 

In addition to following the guidelines set out in this guidance note, there are certain additional actions you may need to carry out, including:

Preparing a privacy risk assessment before installing and using the system to demonstrate that you have made an informed decision about why you have installed the system and how and why it is necessary and appropriate to capture and use data from the cameras. There will be a particular issue if the area includes vulnerable people or those who are required to spend time in the area (e.g. employees).

Preparing a privacy notice which can be viewed by anyone entering the premises, to fully explain who you are, how you intend to use, store and share any data captured by the system and what their legal rights are under the GDPR.

This notice may be presented online and/or maintained for ready access at the front desk. This requirement is in addition to presenting the notices/signage referred to above.

If the camera system impacts **staff** working in the area, you should explain to them directly how the system works. You should also take extra care to ensure the system operates in accordance with applicable employment laws and working practices.

Ensuring you have appropriate processes in place to limit **access** to the cameras to those who need to monitor the system on a 'need to know basis' and only **share** data with others under strict controls.

If you store images, do so in a secure and confidential manner with clear **retention** policies in place to remove or delete safely after an appropriate period of time.

You must respect the **legal rights** that individuals have for example to request access to, delete or restrict use of their data under the GDPR.

You should know who your **data protection supervisory authority** is and be responsible for communicating with them about any concerns or complaints that may be raised in relation to operation of the system, including any data breaches.

Ensure you regularly review the camera system to make sure it is working properly and that you are using it aligned to the principles set out above.



Connect. Prevent. Protect.