**Endava CCTV POLICY (EXCERPT)**

Endava plc and any of its subsidiaries (**Endava**) has established this Close Circuit Television (**CCTV**) Policy (**Policy**) as part of Endava commitment to conducting business in accordance with the highest ethical standards, by observing all applicable laws and regulations in the jurisdictions where we operate. Exceptionally, local CCTV privacy notices may apply, as displayed in our reception desks.

Endava is the controller of the personal data that we process through our use of CCTV in certain of our premises. The ongoing use of existing CCTV in such premises is reviewed periodically to ensure that their use remains appropriate, necessary and proportionate, and that such surveillance system is continuing to address the needs that justified its introduction.

This Policy applies to all Endava employees, as well as contractors and visitors to our premises. We recognize that the images of those individuals recorded by CCTV is personal data and subject to legislation. We use CCTV for our legitimate business interests, including:

* To protect our premises, buildings and assets from damage, disruption, vandalism and crime
* For ensuring the health and safety of our staff, visitors and other members of the public
* To act as a deterrent against crime, to produce necessary evidence and support law enforcement
* To assist in day-to-day management, resolution of disputes, including employment proceedings
* Where in use, to allow biometric recognition of the individuals entering our premises.

CCTV monitors only entrance and exit points in our premises, and certain common areas of our premises inside working hours. Any camera used will be fixed and its capitations are focused oriented (and not panoramic) to minimize viewing of spaces not relevant to the above scope of the monitoring. CCTV cameras will not focus on work areas, private areas, desks, monitors or areas likely to intrude with private personal data. No cameras will be placed in areas where there is an expectation of privacy. CCTV will not be used to record sound.

Live feeds from our CCTV cameras, and CCTV images, are only viewed if required, by authorized personnel only, on a need-to-know basis. Recorded images will only be viewed in designated, secure offices, by authorized staff only. Signs will be displayed near the surveillance zone of any camera to alert individuals that their image may be recorded. Such signs will include details of Endava entity operating the system, purposes (link to this policy), applicable privacy notice (https://www.endava.com/en/Privacy-Notice), and who to contact or complain (Workplace, HR, Legal, privacyenquiries@endava.com).

Data gathered from CCTV is stored to maintain its integrity and security. This may include encrypting. We will never engage in covert monitoring or surveillance of any kind. We may store CCTV video footage using a cloud computing system, in accordance with industry standards. If engaging data processors, contractual safeguards will be in place to protect data security and integrity.

CCTV personal data will be retained for up to 48 hours, and then deleted. Exceptionally, such personal data may be retained for up to 30 days, and then deleted. We will store CCTV personal data longer only when requested by an authority, a legal proceeding or by contract.

We may share CCTV personal data with other Endava group companies if reasonably necessary for the above legitimate purposes. We may allow law enforcement agencies to view or remove CCTV footage where this is required for detection or prosecution of crime. We will maintain a record of all disclosures of CCTV footage. No images from CCTV will be posted online or disclosed to the media.

Individuals, as data subjects, may make a request for disclosure of their personal information and this may include CCTV images **(**data subject access request**),** as per the applicable privacy notice. We recognize that individuals have the right to object to processing, including to prevent processing of their personal data through CCTV. For us to locate relevant footage, any requests for copies of recorded CCTV images must include date and time of recording, location where the footage was captured and, if necessary, information identifying the individual. We will obscure images of third parties when disclosing CCTV data as part of a data subject access request.