

Top management of **CBS Systems d.o.o.** ("CBS") establishes this Information Security Policy and commits to protecting all information assets, its own and those entrusted to it by clients, against every form of threat, internal or external, accidental or deliberate. It does so through the establishment, implementation, monitoring, review, maintenance and continual improvement of an information security management system (ISMS) that meets the requirements of **SRPS ISO/IEC 27001:2022**.

CBS designs, builds, operates and supports enterprise analytics and AI software, including the **SightPulse** decision intelligence platform, which is commercialised by its subsidiary **SightPulse AG** (Zug, Switzerland). In this work CBS processes some of its clients' most commercially sensitive information. Protecting the confidentiality, integrity and availability of that information is the foundation of this policy and of the trust clients place in CBS and SightPulse.

SCOPE

This policy applies to all CBS employees (permanent, temporary and freelance), contractors and other external parties with access to CBS or client information. It covers all processes, systems, locations and remote workplaces used for: the design, development, deployment, operation and support of the SightPulse platform and other CBS software solutions; data engineering, statistical modelling, data science and AI services; and the processing of market and consumer research data.

INFORMATION WE PROTECT

CBS acts as a processor or sub-processor of client data and processes it only on the client's documented instructions. Client information in scope includes:

- **Commercial and financial data:** sell-in, sell-out, point-of-sale and basket, distributor, pricing, promotion, trade terms, cost and margin data;
- **Customer, consumer and shopper data:** CRM, loyalty, e-commerce and digital channel data, which may include personal data;
- **Research and market data:** respondent-level survey, panel and tracker data, and syndicated market data licensed by clients from third parties;
- **Outlet, store, field execution and geographic data,** and product, customer and organisational master data;
- **Models, analyses, segments, forecasts and recommendations** produced for clients, which remain client property.

CBS's own information assets, including source code, models, methods, credentials, infrastructure and business records, are equally in scope.

HOW WE PROTECT INFORMATION

- **Client data stays in the client's environment.** SightPulse is deployed as an Azure Managed Application inside the client's own Azure subscription and tenant, in the region the client selects. Client data is copied to CBS-controlled systems only on the client's written instruction; it is then protected by the same controls and deleted when no longer needed.
- **Least-privilege, accountable access.** Access to client environments is limited to named, trained personnel, protected by multi-factor authentication, logged, and reviewed at defined intervals. Clients choose between standing operational access and just-in-time access that they approve per request.
- **Segregation and purpose limitation.** Each client's data is kept separate and used only to deliver services to that client. It is never used to train or improve models for other clients, and third-party AI providers are not permitted to train on it.
- **Data minimisation.** Personal data is processed only where a use case requires it. Pseudonymised identifiers are preferred and direct identifiers are avoided wherever possible.
- **Encryption** of data in transit and at rest, with controlled management of keys and secrets.
- **Secure development lifecycle.** Security requirements, peer code review, dependency and vulnerability scanning, separate development, test and production environments, and no client production data in development or test without the client's approval.
- **Trustworthy AI.** Statistical and machine-learning models perform the analysis; language models orchestrate and explain. Every output is traceable to its source data and validated before release, and inferred results are flagged as such. Clients may use the language model endpoint their own security team has approved.
- **Supplier security.** Suppliers and subcontractors with access to information are assessed before engagement and bound by confidentiality, security and data protection obligations.
- **Monitoring and incident response.** Security events are logged and monitored. Incidents are reported, investigated, documented and used to improve. Clients are notified of incidents affecting their data without undue delay and within contractually agreed timeframes.
- **Resilience.** Backup, business continuity and disaster recovery arrangements are defined, maintained and tested.

- **People.** Background checks as permitted by law, confidentiality undertakings, security awareness training at onboarding and at regular intervals, and a disciplinary process for violations.
- **Legal and contractual compliance** with the Serbian Law on Personal Data Protection, the EU General Data Protection Regulation and the Swiss Federal Act on Data Protection where they apply, with client contracts and data processing agreements, and with the licence terms of third-party data providers.
- **Return and deletion** of client data at the end of a contract, with written confirmation on request.

OBJECTIVES

- protection of the confidentiality, integrity and availability of client data entrusted to CBS, in every environment where CBS processes it;
- no unauthorised access to client data, and timely detection, containment and notification of any security incident;
- compliance with legal, regulatory and contractual requirements in every jurisdiction where CBS and its clients operate;
- provision of reliable, accurate and traceable information and analytical outputs;
- availability of information and services to authorised users when they need them;
- continual improvement of the ISMS, informed by risk assessment, audits, incidents and client feedback.

Measurable objectives, owners and targets are set in the ISMS objectives register and reviewed at management review.

RESPONSIBILITIES

Top management owns this policy, provides the resources for the ISMS and reviews its performance. ISMS Management Representative coordinates the ISMS, risk assessment and incident management. Every employee, contractor and external party with access to CBS or client information is responsible for complying with this policy and the rules derived from it, within the scope of their role and contract. Non-compliance is handled under the disciplinary procedure of **CBS Systems d.o.o.** and the applicable contracts.

This policy is communicated to all employees and relevant external parties, is available to interested parties, including on sightpulse.ai, and is reviewed at least once a year and whenever significant changes occur.

Belgrade, 2 September 2026

Milan Bjeloglav
Director, CBS Systems d.o.o.



Najviše rukovodstvo **CBS Systems d.o.o.** („CBS“) uspostavlja ovu Politiku bezbednosti informacija i obavezuje se da će štititi svu informacionu imovinu, sopstvenu i onu koju su mu poverili klijenti, od svih oblika pretnji, internih i eksternih, slučajnih ili namernih. To čini kroz uspostavljanje, primenu, nadzor, preispitivanje, održavanje i stalno poboljšavanje sistema menadžmenta bezbednošću informacija (ISMS) usaglašenog sa zahtevima standarda **SRPS ISO/IEC 27001:2022**.

CBS projektuje, razvija, upravlja i podržava softverska rešenja za poslovnu analitiku i veštačku inteligenciju za velike kompanije, uključujući platformu za podršku odlučivanju **SightPulse**, koju komercijalizuje zavisno društvo **SightPulse AG** (Cug, Švajcarska). U tom radu CBS obrađuje neke od komercijalno najosetljivijih informacija svojih klijenata. Zaštita poverljivosti, integriteta i raspoloživosti tih informacija temelj je ove politike i poverenja koje klijenti imaju u CBS i SightPulse.

OBUHVAT

Ova politika se primenjuje na sve zaposlene u CBS-u (stalno, privremeno i honorarno angažovane), ugovarače i druge spoljne strane koje imaju pristup informacijama CBS-a ili klijenata. Obuhvata sve procese, sisteme, lokacije i udaljena radna mesta koji se koriste za: projektovanje, razvoj, implementaciju, upravljanje i podršku platforme SightPulse i drugih CBS softverskih rešenja; inženjering podataka, statističko modelovanje, nauku o podacima i usluge veštačke inteligencije; i obradu podataka tržišnih i potrošačkih istraživanja.

INFORMACIJE KOJE ŠTITIMO

CBS postupa kao obrađivač ili pod-obrađivač podataka klijenata i obrađuje ih isključivo po dokumentovanim uputstvima klijenta. Informacije klijenata obuhvataju:

- **Komercijalne i finansijske podatke:** podatke o prodaji (sell-in, sell-out), podatke sa kasa i o potrošačkim korpama, podatke distributera, cene, promocije, trgovinske uslove, troškove i marže;
- **Podatke o kupcima, potrošačima i kupcima u maloprodaji:** CRM, programe lojalnosti, e-trgovinu i digitalne kanale, koji mogu sadržati podatke o ličnosti;
- **Istraživačke i tržišne podatke:** podatke anketa, panela i trejera na nivou ispitanika, kao i sindikovane tržišne podatke koje klijenti licenciraju od trećih strana;
- **Podatke o prodajnim objektima, prodavnicama, terenskoj realizaciji i geografske podatke,** kao i matične podatke o proizvodima, kupcima i organizaciji;
- **Modele, analize, segmente, prognoze i preporuke** izrađene za klijente, koji ostaju vlasništvo klijenata.

Sopstvena informaciona imovina CBS-a, uključujući izvorni kod, modele, metode, pristupne podatke, infrastrukturu i poslovnu evidenciju, takođe je obuhvaćena.

KAKO ŠTITIMO INFORMACIJE

- **Podaci klijenata ostaju u okruženju klijenta.** SightPulse se instalira kao Azure Managed Application u sopstvenoj Azure pretplati i tenantu klijenta, u regionu koji klijent izabere. Podaci klijenata se kopiraju u sisteme pod kontrolom CBS-a samo po pisanom nalogu klijenta; tada se štite istim kontrolama i brišu kada više nisu potrebni.
- **Pristup po principu najmanjih privilegija, uz odgovornost.** Pristup okruženjima klijenata ograničen je na imenovano, obučeno osoblje, zaštićen je višefaktorskom autentifikacijom, evidentira se i preispituje u definisanim intervalima. Klijent bira između stalnog operativnog pristupa i pristupa „just-in-time“ koji odobrava za svaki zahtev.
- **Razdvajanje i ograničenje svrhe.** Podaci svakog klijenta čuvaju se odvojeno i koriste isključivo za pružanje usluga tom klijentu. Nikada se ne koriste za treniranje ili unapređenje modela za druge klijente, a pružaocima AI usluga trećih strana nije dozvoljeno da ih koriste za treniranje.
- **Minimizacija podataka.** Podaci o ličnosti obrađuju se samo kada to zahteva konkretan slučaj upotrebe. Prednost imaju pseudonimizovani identifikatori, a direktni identifikatori se izbegavaju kad god je to moguće.
- **Šifrovanje** podataka u prenosu i u mirovanju, uz kontrolisano upravljanje ključevima i tajnama.
- **Bezbedan životni ciklus razvoja.** Bezbednosni zahtevi, pregled koda, skeniranje zavisnosti i ranjivosti, razdvojena razvojna, test i produkciona okruženja, i bez produkcionih podataka klijenata u razvoju ili testiranju bez odobrenja klijenta.
- **Pouzdana veštačka inteligencija.** Analizu vrše statistički modeli i modeli mašinskog učenja; jezički modeli orkestriraju i objašnjavaju. Svaki rezultat je sledljiv do izvornih podataka i validira se pre isporuke, a izvedeni rezultati su jasno označeni. Klijent može koristiti jezički model koji je odobrio njegov bezbednosni tim.
- **Bezbednost dobavljača.** Dobavljači i podugovarači sa pristupom informacijama procenjuju se pre angažovanja i obavezuju na poverljivost, bezbednost i zaštitu podataka.
- **Nadzor i odgovor na incidente.** Bezbednosni događaji se evidentiraju i nadziru. Incidenti se prijavljuju, istražuju, dokumentuju i koriste za poboljšanje. Klijenti se o incidentima koji pogađaju njihove podatke obaveštavaju bez nepotrebnog odlaganja i u ugovorenim rokovima.
- **Otpornost.** Rezervne kopije, kontinuitet poslovanja i oporavak od katastrofe definisani su, održavaju se i testiraju.

- **Ljudi.** Provera kandidata u meri u kojoj to zakon dozvoljava, izjave o poverljivosti, obuka o bezbednosti pri zapošljavanju i u redovnim intervalima, i disciplinski postupak za kršenja.
- **Usaglašenost sa zakonima i ugovorima:** sa Zakonom o zaštiti podataka o ličnosti Republike Srbije, Opštom uredbom EU o zaštiti podataka (GDPR) i švajcarskim Saveznim zakonom o zaštiti podataka tamo gde se primenjuju, sa ugovorima i ugovorima o obradi podataka sa klijentima, kao i sa licencnim uslovima dobavljača podataka.
- **Vraćanje i brisanje** podataka klijenata po završetku ugovora, uz pisanu potvrdu na zahtev.

CILJEVI

- zaštita poverljivosti, integriteta i raspoloživosti podataka koje su klijenti poverili CBS-u, u svakom okruženju u kome ih CBS obrađuje;
- nijedan neovlašćeni pristup podacima klijenata, uz blagovremeno otkrivanje, ograničavanje i prijavljivanje svakog bezbednosnog incidenta;
- usaglašenost sa zakonskim, regulatornim i ugovornim zahtevima u svim jurisdikcijama u kojima CBS i njegovi klijenti posluju;
- pružanje pouzdanih, tačnih i sledljivih informacija i analitičkih rezultata;
- raspoloživost informacija i usluga ovlašćenim korisnicima kada su im potrebne;
- stalno poboljšavanje ISMS-a na osnovu procene rizika, provera, incidenata i povratnih informacija klijenata.

Merljivi ciljevi, odgovorna lica i ciljne vrednosti utvrđuju se u registru ciljeva ISMS-a i preispituju na preispitivanju od strane rukovodstva.

ODGOVORNOSTI

Najviše rukovodstvo je vlasnik ove politike, obezbeđuje resurse za ISMS i preispituje njegove performanse. Predstavnik rukovodstva za ISMS koordinira ISMS, procenu rizika i upravljanje incidentima. Svaki zaposleni, ugovarač i spoljna strana sa pristupom informacijama CBS-a ili klijenata odgovoran je za poštovanje ove politike i pravila koja iz nje proističu, u okviru svoje uloge i ugovora. Nepoštovanje se rešava u skladu sa disciplinskim postupkom **CBS Systems d.o.o.** i važećim ugovorima.

Ova politika je saopštena svim zaposlenima i relevantnim spoljnim stranama, dostupna je zainteresovanim stranama, uključujući i na sajtu sightpulse.ai, i preispituje se najmanje jednom godišnje i pri svakoj značajnoj promeni.

Beograd, 02.09.2026.

Milan Bjeloglav
Direktor, CBS Systems d.o.o.

