EGPS
ECONOMIC GROUP
PENSION SERVICES

CYBERSECURITY

Keeping sensitive data safe and secure

At EGPS, we want to assure you we're constantly working to keep our clients' data secure, every single day, every single second – because cyber criminals never sleep.

We've outlined our security practices below, which align with the DOL's recommendations for hiring a service provider.

SECURITY STANDARDS AND THIRD-PARTY VALIDATION

With an industry-leading IT group, EGPS has developed a technology and security plan that is continually reviewed and updated. Its purpose is to ensure EGPS is a leader in the use of technology to support our partners and clients. This includes:

- Optimizing the user experience
- Keeping data secure
- Quickly adjusting to market changes

We make the capital investments necessary to ensure our service is delivered with the highest quality. Our hardware and software platforms were chosen because they are the most successful solutions in the market. Our secure cloud system provides our employees with continuous and secure access to data and computing systems.

EGPS leverages Multi-Factor Authentication (MFA) to ensure only our employees have access to EGPS systems. This security protocol is enabled across multiple software environments. Data in-transit and employee connections to EGPS systems are all encrypted using sophisticated technology to safeguard all data.

The DOL also recommends a third-party audit be completed to validate a service provider's processes and procedures for data security. EGPS is currently in the process of finding and enlisting a third-party agency to review our policies and practices.

HISTORY AND REPUTATION

At EGPS, we have a proven track record of keeping data secure. Our detailed security procedures, systems, and a culture of technology innovation and data security has kept our clients' information safe for over 50 years. Our significant investment in technology and security enables us to provide stellar customer service and support, along with peace of mind.

DISASTER RECOVERY

Safeguarding client databases starts with safeguarding our employees' access to systems. In case of a disaster, we have methods to quickly recover and continue our business services without service interruption. Our security functions include data recovery, data encryption, and protection against the risks associated with the loss of devices.

As part of our security infrastructure, EGPS employees also do not store data on our local computers. If local devices are lost, customer confidential data is not at risk.

ONGOING COMPLIANCE AND TRAINING

End user cybersecurity awareness is paramount to our safe IT operations. We have specific onboarding training protocols to ensure new employees work within our security standards. Additionally, end user training in email phishing and advanced security practices are in the deployment planning stages. From a security automation standpoint, we utilize an active security gateway that runs continuously and secures end users from viruses and phishing attempts.

DEDICATION AND COMMITMENT TO PROTECTING DATA

Our technology training, investment, and culture all have one goal in mind: the best possible experience for our partners and clients. That experience includes:

- Highly responsive communication
- Continuity of services regardless of the situation
- Peace of mind knowing sensitive data is secure

As technology, cyber crimes, and regulations evolve, we're constantly reviewing our systems, processes, training, and policies to continue to ensure we keep our clients' data safe.