Audyt podmiotów przetwarzających

1. **Inspektor Ochrny Danych (IOD)**
   1.1. Czy powołany został Inspektor Ochrony Danych?
   1.2. Kiedy został powołany IOD, data?
   1.3. Czy IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych, kiedy?
   1.4. Czy funkcje IOD pełni pracownik podmiotu, czy jest to firma zewnętrzna?
   1.5. Czy podmiot przetwarzający ma obowiązek powołania Inspektora Ochrony danych?
2. **Dokumentacja ochrony danych osobowych – polityka ochrony danych**
   2.1. Czy wdrożona została dokumentacja ochrony danych i co się na nią składa?
3. **Rejestr czynności przetwarzania (RCP).**
   3.1. Czy prowadzony jest RCP?
   3.2. W jakiej formie jest prowadzony RCP – papierowa/elektroniczna (format Word/Excel)?
   3.3. Czy przyjęty jest proces aktualizacji RCP?
   3.4. Czy prowadzona jest historia aktualizacji dla RCP?
   3.5. Czy przetwarzający korzysta z podwykonawców?
4. **Rejestr kategorii czynności przetwarzania (RKCP).**
   4.1.Czy przetwarzający występuje w roli podmiotu przetwarzającego?
   4.2. Czy prowadzony jest RKCP?
   4.3. W jakiej formie jest prowadzony RKCP – papierowa/elektroniczna (format Word/Excel)?
   4.4. Czy przyjęty jest proces aktualizacji RKCP?
   4.5. Czy prowadzona jest historia aktualizacji dla RKCP?
5. **Analiza ryzyka.**
   5.1.Czy wdrożone zostały odpowiednie środki techniczne i organizacyjne zabezpieczające dane osobowe?
   5.2. Czy przeprowadzono analizę ryzyka dla procesów przetwarzania danych?
   5.3.Kiedy była przeprowadzona ostatnia analiza ryzyka i jakiego procesu przetwarzania danych dotyczyła?
   5.4. Jaki był wynik analizy ryzyka?
6. **Obszar przetwarzania danych.**
   6.1. Czy zdefiniowany jest obszar przetwarzania danych?
   6.2. Czy określono zasady dostępu do obszaru przetwarzania danych (polityka kluczy)?
7. **Procedura postępowania z incydentami i rejestr naruszeń.**
   7.1. Czy określone zostały zasady postępowania z incydentami?
   7.2.Czy prowadzony jest rejestr naruszeń?
   7.3.Czy pracownicy zostali przeszkoleni z zasad postępowania z incydentami?
   7.4.Czy w okresie maj 2018 do grudzień 2023 miały miejsce incydenty?
   7.5.Czy miały miejsce incydenty, które zostały zgłoszone do PUODO?
8. **Prawa osób, których dane dotyczą.**
   8.1.Czy wdrożono procedurę realizacji praw osób, których dane dotyczą?
   8.2.Czy były rozpatrywane wnioski osób, których dane dotyczą, z zakresu przysługujących im praw?
   8.3. Czy prowadzony jest rejestr wystąpień podmiotów danych dot. realizacji ich praw?
9. **Wymiana danych z podmiotami zewnętrznymi.**
   9.1.Czy zawarte są umowy powierzenia?
   9.2.Czy prowadzony jest rejestr podmiotów przetwarzających?

Gmina Piła
Plac Staszica 10
64-920 Piła

9.3.Czy przed zawarciem umowy powierzenia danych przeprowadzany jest audyt podmiotu przetwarzającego, w zakresie niezbędnym RODO?

9.4.Czy dane osobowe są przekazywane poza obszar Unii Europejskiej?

10. Upoważnienia do przetwarzania danych osobowych.

10.1.Czy nadawane są upoważnienia do przetwarzania danych osobowych?

10.2.W jakiej formie są nadawane upoważnienia do przetwarzania danych osobowych?

10.3.Czy prowadzona jest ewidencja osób upoważnionych?

10.4.Czy osoby upoważnione podpisują oświadczenie o zachowaniu danych w poufności?

11. Szkolenia z zakresu ochrony danych osobowych.

11.1. Jak prowadzone są szkolenia z zakresu ochrony danych osobowych (forma/częstotliwość)?

11.2. Jak dokumentowane są szkolenia?

11.3. W jaki sposób weryfikowana jest wiedza pracownika z zakresu ochrony danych osobowych?

12. Obowiązek informacyjny.

12.1.W jaki sposób realizowane są obowiązki informacyjne z art. 13 i 14 RODO?

13. Monitoring wizyjny.

13.1.Czy wprowadzono monitoring wizyjny?

13.2.Czy przyjęty został regulamin monitoringu?

13.3.Jaki obszar objęty jest monitoringiem?

13.4. Czy obszar monitoringu jest odpowiednio oznakowany?

14. Obsługa IT.

14.1. Czy obsługa IT jest wewnętrzna (zatrudniony informatyk) czy zewnętrzna?

14.2. Jakie systemy informatyczne wykorzystywane są do przetwarzania danych osobowych?

14.3. Hosting poczty, hosting strony www - czy są zawarte umowy powierzenia?

14.4. Jakie są zabezpieczenia infrastruktury IT?