Tu je sumarizácia poznatkov z PDF dokumentov do 50 bodov:

1. **Transpozícia smernice NIS2**: Novela zákona o kybernetickej bezpečnosti (ZKB) transponuje smernicu NIS2 v SR2.
2. **Účinnosť novely ZKB**: Zákon č. 69/2018 Z.z. nadobúda účinnosť od 1. januára 20252.
3. **Prechodné obdobie**: Existujúci prevádzkovatelia majú lehotu do 31. decembra 2026 na implementáciu opatrení a auditov2.
4. **Rozdelenie prevádzkovateľov**: Základné a kritické služby2.
5. **Povinnosti**: Analýza rizík a prijímanie opatrení2.
6. **Vzdelávanie**: Povinnosť zvyšovania povedomia o kybernetickej bezpečnosti2.
7. **Hlásenie incidentov**: Bezodkladné hlásenie incidentov2.
8. **Dodávateľský reťazec**: Dôležitosť bezpečnosti dodávateľského reťazca2.
9. **Závažnosť porušení**: Stanovené podmienky pre závažnosť porušení a audity2.
10. **Nezávislosť manažéra**: Zabezpečená nezávislosť manažéra kybernetickej bezpečnosti2.
11. **AI regulácia**: Rámec pre zlepšovanie, etiku a reguláciu AI2.
12. **AI Act**: Nové európske právne regulácie týkajúce sa AI4.
13. **AI systém definícia**: Strojový systém schopný generovať predpovede a rozhodnutia4.
14. **Obavy**: Legálnosť, presnosť výstupov, zodpovednosť, súkromie, duševné vlastníctvo, kybernetická bezpečnosť4.
15. **Slabé stránky LLM**: Falošné tvrdenia a halucinácie4.
16. **Klasifikácia AI systémov**: Podľa úrovne rizika4.
17. **Zakázané praktiky**: Systémy AI, ktoré predstavujú jasné hrozby4.
18. **Vysokorizikové systémy**: Vyžadujú si prísne dodržiavanie predpisov5.
19. **DPIA vs. FRIA**: DPIA zamerané na ochranu práv jednotlivcov, FRIA na riadenie rizík pre organizáciu1.
20. **Normy pre DPIA**: Napr. ISO/IEC 291341.
21. **Kyber-bezpečnosť AI systémov**: Požiadavky vyplývajúce z AI Act, ZKB/NIS2 a GDPR3.
22. **Systémy riadenia rizík**: Vysoko-rizikové AI systémy musia implementovať systémy riadenia rizík3.
23. **Dátová governance**: Zabezpečenie dátovej governance3.
24. **Technická dokumentácia**: Požiadavka na technickú dokumentáciu3.
25. **Technológie na zaznamenávanie**: Používanie technológií na zaznamenávanie a dotazovanie3.
26. **Riziká AI**: Identifikácia a riadenie špecifických rizík ako otrávenie modelov3.
27. **AI v recruitmente**: Integrácia AI v nábore, dôležitosť pre efektivitu6.

28. **AI literacy**: Dôležitosť AI literacy6.
29. **Kvalita dát**: Udržiavanie kvality dát6.
30. **Ľudský dohľad**: Potrebný ľudský dohľad na zmiernenie zaujatosti6.
31. **Súlad s právnymi predpismi**: Zváženie súladu s právnymi predpismi pri používaní AI v recruitmente6.
32. **Výber poskytovateľov AI**: Výber poskytovateľov AI s podrobnou dokumentáciou o riadení rizík a transparentnosti6.
33. **Opatrenia na prevenciu zaujatosti**: Ľudský dohľad, kvalita dát, zabezpečenie spoľahlivosti a kybernetickej bezpečnosti, dokumentácia a transparentnosť6.
34. **Legislatívny rámec**: Kľúčové právne normy ako NIS 2, DORA a nový AI Act5.
35. **Zmluvy s IKT poskytovateľmi**: Potrebné na ochranu osobných a firemných dát1.
36. **Zmluvné dojednania**: Úprava práv a povinností, zodpovednosť za bezpečnosť, podmienky auditu a reakcie na bezpečnostné incidenty1.
37. **Povinnosti prevádzkovateľov**: Povinnosť uzatvárať zmluvy so zabezpečením bezpečnostných opatrení a podrobením sa dohľadu1.
38. **Výnimky z AI Act**: AI systémy, ktoré nepredstavujú významné riziko ujmy, môžu byť vyňaté z niektorých požiadaviek6.
39. **Podmienky pre výnimky**: Úzko vymedzená procedurálna úloha, zlepšenie výsledku ľudskej práce, zisťovanie vzorcov rozhodovania6.
40. **Webscraping**: Zohľadnenie aspektov webscrapingu a zabezpečenie ochrany osobných údajov pri vstupoch a výstupoch AI systémov6.
41. **Školenia užívateľov**: Dôležitosť školenia užívateľov AI systémov6.
42. **Zodpovednosť dodávateľov**: Riešenie zodpovednosti dodávateľov AI systémov6.
43. **Etické úvahy**: Zohľadnenie etických úvah pri nasadení AI6.
44. **Monitorovanie a hodnotenie**: Monitorovanie a hodnotenie výkonu a správania na pracovisku pomocou AI4.
45. **Zodpovednosť za obsah**: Otázky zodpovednosti za obsah generovaný AI systémami4.
46. **Príčinná súvislosť**: Zložitosti pri preukazovaní zavinenia a príčinnej súvislosti pri chybách AI4.
47. **Riadenie rizík**: Potreba systémov riadenia rizík počas celého životného cyklu AI systémov5.
48. **Kvalita dát**: Zabezpečenie kvality dát a minimalizácia zaujatosti5.
49. **Transparentnosť**: Transparentnosť a jasné užívateľské inštrukcie5.
50. **Kybernetická bezpečnosť**: Význam opatrení kybernetickej bezpečnosti na ochranu pred neoprávneným prístupom a zraniteľnosťami systému5.